Diocese of Grand Rapids
Acceptable Use Policy Office of Catholic Schools

Electronic Information Access and Acceptable Use of School Systems
Purpose

The Roman Catholic Diocese of Grand Rapids encourages and strongly promotes the use of electronic information technologies in our ministries. As a Catholic organization we have been charged to embrace technology as a way to connect with an online community bringing the message of Jesus Christ and reflecting his character to the world.

Immaculate Heart of Mary Catholic School (the "School") encourages and strongly promotes the use of electronic information technologies in educational endeavors. The School provides access to electronic information resources in a variety of formats, and for the development of information management skills. Together these allow learners to access current and relevant resources and provide the opportunity to communicate in a technologically rich environment and assist them in becoming responsible, self-directed, lifelong learners.

The School has developed this Electronic Information Access and Acceptable Use of School Systems policy (this "Policy") to govern the access, use and security of School Systems (defined below). Every User (defined below) must read, sign and abide by this Policy.

For the purposes of this Policy, the following capitalized terms have the meanings ascribed to them below. Additional capitalized terms are defined within this Policy.

(a) "PEDs" means portable electronic devices, including, without limitation, laptop computers, cellular telephones, pocket personal computers, handheld computers, cameras, video recorders, sound recording devices and all forms of portable electronic devices.

(b) "School Confidential Information" means all confidential and/or proprietary information and materials of the School, its faculty, administrators, students, employees, volunteers and/or third parties with which the School does business.

(c) "School Electronic Information" means all electronic information (including the School Confidential Information), communications or activity created, sent, received, stored and/or otherwise used on behalf of the School, whether or not the School Systems are used to create, send, receive, store or otherwise use that information or those communications. The School Electronic Information includes voicemail messages on the School Equipment.

(d) "School Equipment" means any and all electronic devices owned, leased or operated by or for the benefit of the School, which have the capability of creating, sending, receiving, storing and/or otherwise using electronic information, materials and/or communications, including, but not limited to, pagers, computers, servers, disk drives, scanners, photocopiers, printers, fax machines, telephones and PEDs. School Equipment includes all operating software, application software and firmware owned and/or licensed by the School, which resides and/or is embedded in any the School Equipment.

(e) "School Networks" means all School voice and data systems, including, without limitation, the School's Internet, intranet and extranet systems.

(f) "School Systems" means the School Equipment and the School Networks.

(g) "Users" means any individual who accesses and/or uses School Systems, including, without limitation: (i) School full time, part-time and temporary faculty and/or employees; (ii) School third party contractors, vendors, consultants, representatives and agents, as well as their full time, part-time and temporary employees; and (iii) parents, students and volunteers.

(h) "User Equipment" means electronic devices that are continuously or intermittently connected to School Systems, or a component thereof, which are not owned or leased by the School, including, without limitation, User-owned computers, pagers, telephones, fax machines and PEDs. User Equipment without connectivity to School Systems does not fall under the purview of this Policy.

Scope

This Policy applies to all Users and to all School Systems, User Equipment, School Confidential Information and School Electronic Information.

To the extent this Policy applies to School faculty and/or employees, and volunteers, this Policy supplements, but does not replace, the School's Parent & Student Handbook. The terms of this Policy will govern any conflict or inconsistencies with the terms of such Parent & Student Handbook. Any School faculty and/or employee who violate this Policy may be subject to disciplinary action, up to and including termination.

To the extent this Policy applies to students, this Policy supplements, but does not replace, the School's Parent & Student Handbook. The terms of this Policy will govern any conflict or inconsistencies with the terms of such Parent & Student Handbook. Any student who violates this Policy may be subject to disciplinary action, up to and including suspension and/or expulsion.

To the extent this Policy applies to third parties, this Policy supplements, but does not replace, School's agreements with such third parties. The terms of this Policy will govern any conflict or inconsistencies with the terms of such agreements. Third parties who violate this Policy may no longer be considered eligible for access to and/or use of School Systems, School Confidential Information and/or School Electronic Information. A third party's violation of this Policy shall also be considered a material breach of its agreement with School, entitling School to terminate such agreement for cause.

Policy

The School Systems, School Confidential Information and School Electronic Information are the School's property and may be used solely for educational purposes and/or the School's operational activities. Each User must take all necessary steps to prevent unauthorized access to or use of School Confidential Information and School Electronic Information. Unless otherwise directed by School, or permitted or required by this Policy, Users may not: (a) take, retain or use School Confidential Information and/or School Electronic Information for User's own benefit; (b) disclose School Confidential Information and/or School Electronic Information to any other entity or unauthorized person without the written permission from a School officer; (c) delete, encrypt, password protect, or retain electronic files containing School Confidential Information and/or School Electronic Information (including emails and attachments); or (d) take any other action that impairs, restricts, limits, or impedes School's ability to have full access to and use of its School Confidential Information and/or School Electronic Information. Upon request, User shall return to School all School Confidential Information and/or School Electronic Information, and otherwise fully cooperate with and assist School in ensuring School's ability to have full access to and use of School Confidential Information and/or School Electronic Information. Such cooperation and assistance may include, but is not limited to, removing any password protection, encryption or other proprietary format on School Confidential Information and/or School Electronic Information.

The School retains the right to search, monitor, access and/or review all School Systems, School Electronic Information and all other electronic and voice mail communications, computer files, databases and any other electronic transmissions contained in or accessed by School Systems, at any time, with or without notice, at School's sole discretion. This may include, without limitation: (a) viewing, printing, downloading and/or listening to emails and voicemails created, sent, received, stored and/or otherwise used in or through School Systems; (b) viewing, modifying and/or removing a User's electronic mailbox; and/or reviewing audit trails created by School Systems.

No email, voicemail or other information, whether received, sent, stored or used on or through School Systems, is private. Users have no expectation that any information contained on any School Systems is confidential or private to them. The School's System is not a public forum and access to the technology is a privilege and not a right. By using School Systems, Users consent to the access and disclosure of email messages, voicemail messages and other information within School's organization without restrictions, but subject to School's legal and contractual obligations of confidentiality. Users should not use School Systems to create, send, receive and/or store information that is personal if it is confidential or sensitive, since such personal information will be considered School Electronic Information if created, sent, received and/or stored using School Systems.

The School makes no warranties of any kind, whether expressed or implied, for any reason regarding the access to, or use, quality or availability of, School Systems, including but not limited to the loss of data. All School Systems are provided on an *"as is, as available"* basis.

School Responsibility

Internet Safety Provisions

The School will designate a system administrator who will manage the School Systems and make the final determination as to what is inappropriate use based on this Policy. The system administrator will designate a back-up system administrator in the event that the system administrator is not available. The system administrator or the back-up system administrator may close an account at any time for infractions or temporarily remove a User account and/or a User's access to or use of the School Systems for any reason, including, without limitation, to prevent unauthorized activity.

The School will implement filtering software intended to block access to materials that are obscene, child pornography, harmful to minors, or that the School determines to be inappropriate for minors. However, the School does not guarantee that it will be able to fully prevent any User's access to such materials, or that Users will not have access to such materials while using School Systems. The filtering software will operate on all School Equipment which have Internet access while at school or outside of the School's Networks and on all User Equipment within the School wide area network (WAN) or local area network (LAN).

Subject to system administrator approval and staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

The School does not take responsibility for resources located or actions taken by any Users that do not support the purposes of the School.

It shall be the responsibility of all members of the School staff to supervise and monitor usage of the School Network and access to the Internet in accordance with this Policy and the Children's Internet Protection Act.

The school will implement education about online safety and appropriate online behavior. This education includes, but is not limited to, interacting with other individuals on social networking websites and chat rooms and cyberbullying awareness and response.

Immaculate Heart of Mary Catholic School Network Users

Users will be granted access to appropriate services offered by the School Network. In addition, the following people may become account holders or members of the School Network:

1. Students. Students who are currently enrolled in the School may be granted a School Network account upon agreement to the terms stated in this Policy.

2. Faculty and Staff. Staff members currently employed by the School may be granted a School Network account upon agreement to the terms stated in this Policy.

3. Others. Anyone may request a special account on or use of the School Network. These requests will be granted on a case-by-case basis, depending on need and resource availability.

Privileges and Responsibilities of Users

Privileges

Subject to the terms of this Policy, Users have the privilege to:

1. use all authorized School Systems for which they have received training to facilitate learning and enhance

educational information exchange and/or assist with performance of job responsibilities.

2. access information from outside resources which facilitate learning and enhance educational information exchange and/or assist with performance of job responsibilities.

3. access School Networks and the Internet to retrieve information to facilitate learning and enhance educational information exchange and/or assist with performance of job responsibilities.

Responsibilities

Users are responsible for:

1. using School Systems only for facilitating learning, appropriate personal growth and enhancing educational information exchange consistent with the purposes of the School.

2. attending appropriate training sessions in the use and care of School Systems.

3. seeking instruction for the use of any available technology with which they are not familiar.

4. adhering to the rules established for the use of School Systems, in the School or through remote access outside of the School.

5. refraining from disclosing, using or disseminating personal identification information regarding students over the Internet without parent or guardian authorization.

6. maintaining the privacy of passwords and are prohibited from publishing or discussing passwords. School Network accounts are to be used only by the authorized owner of the account for the authorized purposes. students may use email, chat, instant messaging, and other forms of two-way electronic communications only for educational purposes and only under the direct supervision of an adult.

7. having all electronic media scanned for virus, dirt, damage or other contamination which might endanger the integrity of School Systems before they are used in School Systems.

8. material received, created or distributed using School Systems.

9. maintaining the integrity of the electronic messaging system (voice, email, etc.), deleting files or messages if they have exceeded their established limit, reporting any violations of privacy and making only those contacts which facilitate learning and enhance educational information exchange. If a User remains in noncompliance, the system administrator may delete files and messages, freeze the account, and/or close the account.

10. preventing material considered pornographic by the School, inappropriate files or files dangerous to the integrity of the School's Systems from entering the School via the Internet or from being reproduced in visual, digital or written format.

11. awareness of and adherence to copyright laws and guidelines and trademark laws and applicable licensing agreements in the use of School Systems and in the transmission or copying of text or files on the Internet or from other resources. Users must also comply with all other applicable laws, both state and federal, with respect to their use of the School’s Systems.

12. using caution (*Buyer Beware*) when considering the purchase of goods or services over the Internet. The School is not liable for any financial obligations made nor any personal information provided while using School Systems.

13. financial restitution for unauthorized costs incurred or damages or repair necessitated by inappropriate use or access.

14. any damages to, or incurred on, User Equipment. Users accessing School Systems on User Equipment do so at their own risk.

15. abiding by the rules set forth in this Policy, general School rules, and additional rules as may be established by the School. Local School Committee policies, staff manuals, departmental procedures, and student handbooks may include such rules.

Users are prohibited from:

1. using the technology for a “for-profit” business, for product advertisement or political lobbying.

2. the malicious use of technology to disrupt the use of technology by others, to harass or discriminate against others or to infiltrate computer systems or files without proper permission and authorization (hacking).

3. accessing, using, disclosing or disseminating personal identification information about minors.

4. using School Systems to draft, send, or receive inappropriate communications and material including but not limited to, items which might be considered as pornographic, obscene, profane, vulgar, harassing, threatening, defamatory, bullying or are prohibited by law.

5. participating in hate mail, harassment, discriminatory remarks and other antisocial/bullying behaviors on the network.

6. vandalizing School Systems or any other information technologies (the School's or any others). Vandalism is defined as any attempt to harm, destroy, or disrupt or hack the operation of the School's Systems. Vandalism includes, but is not limited to, the creation or intentional receipt or transmission of computer viruses.

Social Media Use

All communication with minors (in person, via social media, websites, text messages, etc.) must adhere to:

- The Charter for Protection of Children and Young People
- The Children’s Online Privacy and Protection Act
- The Diocesan Office of Child and Youth Protection policies

With the continuing evolution of new media and next generation communications tools, the way in which our parishes, schools and families can communicate internally and externally continues to develop at a rapid pace. While this creates new opportunities, it also creates new responsibilities.

Electronic communication with minors must not be undertaken lightly. School, parish and other Affiliate Employees and Volunteers must consistently adhere to Catholic values and transparency with respect to such communications.

Many Web 2.0 tools commonly used for instruction have social media components to them which allow for sharing, collaboration and commenting. Some of these sites can be set up for a particular classroom or group, thus limiting comments to recognized participants. Others are more public in nature, allowing interaction from a wider audience. The following guidelines have been established to provide a framework for successful and beneficial use of opportunities afforded by such tools.

Schools receiving federal funding for computer technology through E-Rate must comply with the Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5), which requires monitoring internet use by minors; filters to restrict access to obscenity, child pornography, or other material harmful to minors; and educating minors about appropriate online behavior, social networking safety, and cyberbullying.

In light of Immaculate Heart of Mary Catholic School’s mission to create a Catholic culture for instruction and faith formation and out of respect for the primary role that parents have as the first educators of their children, the following guidelines have been established to provide a framework for successful and beneficial use of opportunities afforded by such tools.

General Standards for Staff and Volunteers:
It is the responsibility of the organization and staff members to know and adhere to the standards reflected in the Social Media Policy established by the Diocese of Grand Rapids. When communicating with minors:

1. Use of communication tools between adults and minors should be confined to content that is ministerial / educational in nature and directly relates to the work around the subject matter at hand.
2. Use of communication tools between adults and minors such as instant messaging, chat, email, or text messaging for topics that are personal or that do not relate to ministerial / educational work are prohibited.
3. Do not accept friend or follow requests from minors on your personal accounts.
4. While it is understood that faculty/staff may use communication tools outside of conventional work hours to fulfill professional obligations such as responding to email, facilitating forum discussion or blog commentary. Each staff member will define the norms for electronic communication in his or her setting.
5. It is the responsibility of the staff member to set the proper security guidelines and monitor social media tools as used for educational / ministerial purposes, as well as instruct minors in appropriate use.

General Standards for Minors:
It is the responsibility of the user to utilize tools in a responsible manner that adheres to Acceptable Use Policy and the Code of Conduct established by Immaculate Heart of Mary Catholic School.

1. You are a representative of your family, your Church and your school. Bring pride to each of these important aspects of your life.
2. Following, linking, or “friending” official professional social media accounts of the parish / school and is acceptable and encouraged.
3. Following, linking, or “friending” personal accounts of adults is not acceptable.
4. Respect all people, whether you know them or not. Keep all chat positive.
5. Be careful about "kidding" and "joking". Not everyone will see it as kidding and/or joking.
6. Ask permission before posting photos and video of others; remove photos and videos of others if requested.
7. While it is understood that users may use communication tools outside of conventional hours to participate in programs; i.e., email, research, etc. users should exercise a balanced approach to online interaction.

General Standards for Parents / Guardians
It is the responsibility of parents / guardians to be aware of social media use by their children and to communicate with the parish, school or affiliate organization if they have concerns. For additional resources, visit our website at: https://ihmschoolgr.org

1. Establish clear guidelines for use in the home (i.e., hours of disconnect or charging a device in a common area not stored in the bedroom overnight)
2. Participate with your children in their online activities;
    2.1. know and follow your children on Instagram, Twitter and other social accounts
    2.2. read and comment on program blogs
    2.3. play a game across the room
3. Following, linking, or “friending” official professional social media accounts of the parish / school and is acceptable and encouraged.
4. Model and support responsible use as outlined here and in the Acceptable Use Policy.

Declaration -- All users are required to sign this form. *All minors are considered users and will require the signature of a parent or guardian in the space provided at the bottom of the page. Due to the nature and complexity of the policy, minors in grades K-6 will not be required to sign the form; however, minors in grades 7-12 must read and sign the form in addition to their parent(s) or guardian(s).*

The School has developed this Policy for all Users and it applies to all School Systems, User Equipment, School Confidential Information and School Electronic Information. Access and use of School Systems is a privilege for each User.

I have read, understand and will abide by this Policy. I agree to be responsible for and abide by this Policy and all other rules, regulations, policies and/or procedures related to School Systems. I understand that should I commit any violation, my privileges and/or account may be revoked, and that disciplinary action and/or appropriate legal action may be taken.

I understand and acknowledge that I might locate material that could be considered offensive or controversial, that parents of minors should be aware of the existence of such materials and monitor home usage of School Systems, and that students knowingly bringing or downloading such material into the School environment will be dealt with according to the discipline policies of the School.

In consideration for the privilege of using the School Systems and in consideration for having access to the information contained or accessed on it, I hereby release the School and its operators and sponsors, its faculty and staff and all organizations, groups and institutions with which the School is affiliated for any and all claims of any nature arising from my use, my child's use or inability to use, the School Systems.

User's Signature:_____

Print User's Name: _____

Date: _____

Parent or Guardian (only needed for users under the age of 18)

As the parent or guardian of this minor, I have read this Policy and understand that this access is designed for legitimate educational purposes. The School has taken precautions to prohibit access to inappropriate materials. However, I also recognize it is impossible for the School to restrict access to all inappropriate or copyrighted materials and I will not hold them responsible for materials acquired on or through the School Systems or any consequences of such acquisition of materials. Further, I accept full responsibility for supervision if and when my child's use of any School Systems is not in a school setting.

Users are responsible for attending appropriate training sessions in the use and care of all School Systems and should refrain from using any technology for which they have not received training.

Users may be required to make full financial restitution for any damages to School Systems or unauthorized expenses incurred through the use of School Systems.

As the lawfully authorized parent or guardian of the minor identified above, I hereby give permission to issue a membership account to this individual.

Parent/Guardian Signature: _____

Print Parent/Guardian Name: _____

Date: _____