

# Greater Muskegon Catholic Schools

## Acceptable Use Policy

### For Students in Grades 5 – 12

#### Rights and Responsibilities

Access to the GMCS network and Internet is a privilege. All students and staff must agree to the following policies in order to use the computer network at Greater Muskegon Catholic Schools.

Students and staff members should expect only limited privacy in the contents of their personal files on the GMCS network. Routine maintenance and monitoring of the network/Internet may lead to discovery of a violation of a GMCS policy or the law. Intent to violate policy will be considered the same as an actual policy violation.

#### **Rights:**

All GMCS students and staff have the right to make educational use and limited personal use of all hardware and software authorized for their use and for which they have received training.

GMCS staff members have e-mail access through the school network. This e-mail is not guaranteed to be private and must conform to the rules established by GMCS, MAISD, and Merit, Inc.

GMCS students do not have access to an e-mail account through the school network, but may subscribe to an appropriate free web-based e-mail service. Students must comply with all GMCS policies when using an e-mail account via the school network.

#### **Responsibilities:**

All GMCS students and staff:

- must have a signed Contract Agreement on file with the Director of Technology before being allowed access to the GMCS network or the Internet.
- are responsible for the care and proper use of hardware and software. Any damages that occur to hardware and/or software because of improper use are the financial responsibility of the user.
- are responsible for printing documents of a reasonable length. Printing excessive printing may require financial reimbursement.
- are not to use hardware or software for private business, product advertisement, or political activities.
- are not to download, install, remove, relocate, or modify any hardware or software. This includes attempting to gain unauthorized access to system programs or computer equipment.
- are not to use anonymous proxies or other software in an attempt to hide Internet activity or access blocked websites.

- Users are responsible for any civil liabilities and criminal penalties resulting from violations of copyright laws or software licensing agreements.
- Are not to connect non GMCS-owned hardware to the network without permission from the Director of Technology.
- shall not engage in activities that are intended to hinder another's ability to use the network. Educational use always has priority over personal use.
- are responsible for the confidentiality of their passwords as well as the use of technology through that password.
- are to respect the privacy of others. This includes not reading, copying, changing or using other's files or trying to learn, change, or use their passwords.
- shall not attempt to gain unauthorized access to the GMCS Network or Internet or to any other computer system or go beyond authorized access, even for the purpose of "browsing."
- are responsible to keep programs of a viral nature off any school equipment. The user will be held accountable for any deliberate attempts to knowingly install and/or run a computer virus.
- are responsible for removing unneeded files and mail in a timely manner and to limit the amount of material downloaded to the school computers. Student files will be removed at the end of each school year.
- are responsible for all activity during their login session and are not to leave their station unattended for any reason. Users must properly log out at the end of their session.
- shall use appropriate language on the GMCS network and Internet. Hate mail, harassment, discriminatory remarks, intimidation, profanity, and other antisocial behaviors are prohibited.
- shall not intentionally misrepresent themselves. This includes seeking, obtaining, or modifying unauthorized information.
- are not to give out personal information about themselves or others (name, address, phone, etc).
- are responsible for all files received via the Internet. It is the responsibility of students and staff to make sure no copyrighted software, pornographic material, inappropriate files, or files known to carry harmful viruses enter the school via the Internet.
- are responsible for keeping images/text/video containing pornographic material or material otherwise inappropriate for school use from being viewed or printed.
- shall adhere to the values of our Catholic community when judging the appropriateness and content of material they access, transmit, publish or store on the network.
- shall not encrypt any files stored on the GMCS network.
- are responsible for not using the GMCS network for games, messaging or electronic chatting of any form.
- are not to download/stream audio or video files. This limits the available bandwidth and may violate copyright laws.

- Are not to connect to the GMCS network any personal computer or other device without prior permission of the GMCS Technology Department. This prohibition includes, but is not limited to, laptop computers, gaming devices, storage devices, telephones, PDAs, digital cameras, and MP3 players. The GMCS Administration and/or Technology staff reserves the right to inspect the contents of such devices at any time.
- are to respect the rights of copyright owners, not use material from the Internet for plagiarism, and must not make unauthorized copies of software or media protected by copyright laws.
- are responsible for adhering to the rules established for hardware and software use by the Technology Department or the teacher/supervisor in charge of the library/media center, computer lab, or classroom.

This policy is updated periodically. Your signature on this Acceptable Use Policy is binding for subsequent Acceptable Use Policies. A copy of the most recent AUP is available at <http://www.gmcs.org>. Use of your account signifies your agreement with the updated policy.

## **Policy Enforcement Guidelines**

Depending on the nature and severity of the policy violation and existing student handbook procedures regarding inappropriate behavior, the technology instructor or school administrator may take one or more of the following disciplinary actions:

- a. Verbal or written warning
- b. Temporary access denial
- c. Permanent access denial
- d. School suspension
- e. Expulsion
- f. Alternative punishment

Demonstrated intent to violate policy will be considered the same as an actual policy violation. Demonstrated intent means evidence of actions that if successful or if carried out as intended, would result in a policy violation.

Evidence of attempted or actual system security, integrity, or performance-related incidents will be cause for immediate access denial.

If warranted, the school administrator will refer the case to Local, State, or Federal authorities for further disposition.