

# Greater Muskegon Catholic Schools

## Acceptable Use Policy

### For Students in Grades K – 4

#### Rights and Responsibilities

Through the GMCS network, we are pleased to provide network services for student access to educational resources, to present information and to work collaboratively with peers and experts. These services are provided as a privilege. All students and staff must agree to the following policies in order to use the computer network at Greater Muskegon Catholic Schools.

There are networked computers (networked meaning the computers that are connected to the Internet, as well as shared resources on a server) accessible to students in classrooms, computer labs and libraries.

#### User Responsibilities - "Do's and Don'ts"

- Do use the network according to the school's code of conduct.
- Do use the network only for legal activity.
- Do print school work only. Outside school work/printing is allowed by permission of your teacher.
- Do use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
- Do use the Internet only when you have permission from a teacher.
- Do not cut and paste information from the Internet as your own work.
- Do not access or change in any way another person's work.
- Do not gain or attempt to gain unauthorized access to resources or information.
- Do not log into the computer without permission.
- Do not damage or mistreat computer equipment under any circumstances.
- Do not copy, download or install any software or programs to school computers. Do not remove, relocate or modify hardware or software.
- Do not download or stream audio/video files. This limits everyone's use of our computer network.
- Do not use anonymous websites or other software in an attempt to hide Internet activity or visit blocked websites.
- Do not connect to the GMCS network any personal computer or other equipment without permission from the technology staff. This 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 this equipment at any time.

#### Personal Safety

- Report to your teacher or other adult any security problems, or information that makes you uncomfortable.
- Do not give out your home address, picture or phone number or those of other students or staff. Use school addresses and phone numbers only, and only with permission from an adult staff member.

## **Inappropriate Use**

The students are responsible for their actions and activity during their login. Unacceptable uses of the network will result in the suspension or revoking of these privileges. Students will be referred to GMCS staff for disciplinary action.

Students should follow the values of our Catholic community when judging the appropriateness and content of material they access, transmit, publish or store on the network.

Students 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 that a GMCS policy or law has been violated. Intent to violate policy will be considered the same as an actual policy violation.

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 a student 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 teacher 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 needed, the school administrator will refer the case to Local, State, or Federal authorities for further investigation