STUDENT TECHNOLOGY USE AGREEMENT

These administrative rules apply to all persons accessing and using electronic network systems owned, leased, or allowed by a school in the Diocese of Davenport. These persons include students, faculty, staff, and user privileges extended by the school. A user does not own his/her network accounts but does have access to the accounts. Access to computing resources is a privilege, not a right. It is a privilege that the local school extends to users who are trusted to make responsible use of computing resources.

The user agrees to:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behavior that is expected offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff members if he/she sees bullying/threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Be cautious to protect the safety of self and others.
- Help protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgement when using school technologies. The following violations may lead to disciplinary action or loss of Network privilege or both. This list includes but is not limited to the following:

I will not

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Place illegal, or inflammatory material on the Internet in the form of e-mail or web pages.
- Give my password to another user.
- Pose or try to log in as a network user other than myself.
- Attempt to post messages or sign up with a public USENET group or ListSERV without the authorization of a teacher or network administrator.
- Create or spread computer viruses.
- Forward messages that would be considered obscene or unacceptable by the standards of the local school.
- Download applications, executables, or installers without permission of the network administrator.
- Use electronic communication to inform other students or give them information about tests, answers to quizzes, or other information that would be considered cheating.
- Copy software without the written permission of the software manufacturer.
- Attempt to hack into a server, computer, or network inside or outside of the local school.
- Vandalize any network hardware, software, printers, computers, keyboards, etc.
- Pose or try to log in as a network administrator.
• Use another person’s name or password to access Internet or e-mail.
• Let another user use my network account, with or without permission.
• Try to break the security system or bypass safeguards put in place by the local school.
• Mail bomb or purposefully overload another user or system using e-mail.
• Connect to any site involving gambling, alcohol, or drugs.
• Access chat rooms of any kind without the permission of a staff member.
• Send pictures that are personably identifiable without permission.
• Send abusive messages to others or use inappropriate language.
• Play online games without the permission of the teacher.
• Use local school resources for political lobbying.
• Engage in cyberbullying, harassment, or disrespectful conduct toward others, staff or students.
• Plagiarize content I find online or break copyright rules or laws.
• Try to find ways to circumvent the school’s safety measures and filtering tools.
• Use school technologies to send spam or chain mail.
• Post another student’s work without that student’s consent or knowledge or post information anonymously.
• Use the internet from the local school for commercial purposes or product advertisement.
• Use or attempt to use proxy servers to bypass filtering mechanisms put in place by the local school.
• Access, download, store copy or print files that are profane or obscene.
• Post personally identifying information, including phone numbers and addresses, about myself or others without permission.
• Agree to a personal encounter with someone who contacted me online.
• Use school technologies for illegal activities or to pursue information on such activities.
• Attempt to hack or access sites, servers, accounts, or content that isn’t intended for my use.
• Modify in any way the hardware or software owned or leased by the local school.

A copy of this signed agreement should be kept by the local computer system administrator.

I understand and will abide by the above acceptable use policy. I further understand that any violation of the policy is unethical and may constitute a criminal offense that may result in the revocation of privileges, disciplinary action and/or legal action.

User’s Full Name: _______________________________ Signature: __________________ Date: ____/____/____

If the user is under age 18, a parent or guardian must also sign below:

Parent or Guardian: I understand the acceptable use policy and hereby give permission to issue an account for my child and certify that the information given on this form is correct.

Name: _______________________________ Signature: __________________ Date: ____/____/____