

Great Falls Central Catholic High School
Print, sign and return the last page of this document

Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prescribed behavior by users, however, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Terms and Conditions

1. Acceptable Use - Access to the school's electronic networks must be (a) for the purpose of education or research and consistent with educational objectives; or (b) for legitimate business use.

2. Privileges - The use of the school's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The building principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His/her decision is final.

3. Unacceptable Use - The user is responsible for his/her actions and activities involving the network. Some examples of unacceptable uses are:

1. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U. S. or state law;

2. Unauthorized downloading of software, regardless of whether it is copyrighted or devirused;

3. Downloading copyrighted material for other than personal use;

4. Using the network for private financial or commercial gain;

5. Wastefully using resources, such as file space;

6. Hacking or gaining unauthorized access to files, resources, or entities;

7. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;

8. Using another user's account or password;

9. Posting material authorized or created by another, without his/her consent;

10. Posting anonymous messages;

11. Using the network for commercial or private advertising;

12. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing or illegal material; and

13. Using the network while access privileges are suspended or revoked.

4. Network Etiquette - The user is expected to abide by the generally accepted rules of network

etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in messages to others.
2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
3. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
4. Recognize that electronic mail (e-mail) is private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
5. Do not use the network in any way that would disrupt its use by other users.
6. Consider all communications and information accessible via the network to be private property.

5.No Warranties - The school makes no warranties of any kind, whether expressed or implied, for the service it is providing. The school will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The school specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6.Indemnification - The user agrees to indemnify the school for any loss, costs, or damages, including reasonable attorney fees, incurred by the school, relating to or arising out of any violation of these procedures.

7.Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

8.Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action.

Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

9. Telephone Charges - The school assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

10.Copyright Web Publishing Rules - Copyright law prohibits the republishing of text or graphics found on the Web or file servers, without explicit written permission.

- 1.For each republication (on a Web site or file server) of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.

- 2.Students and staff engaged in producing Web pages must provide library media

specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the statute of "public domain" documents must be provided.

3. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.

4. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

5. Student work may only be published if there is written permission from both the parent/guardian and the student.

Internet Safety

1. Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses", as detailed in these procedures, and will otherwise follow these procedures.

2. Staff members shall supervise students while students are using Internet access, to ensure that the students abide by the terms and conditions for Internet access, as contained in these procedures.

3. Each school computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene; (2) pornographic; or (3) harmful or inappropriate for students, as defined by the children's Internet Protection Act (CIPA)

4. The building principals shall monitor student Internet access

5. Legal Reference: Children's Internet Protection Act, P.L. 106-554 20 U.S.C. § 6801, et seq.
47 U.S.c. § 254(h) and (1)

STUDENTS

Access to Electronic Information, Services, and Networks

General

Internet access and interconnected computer systems are available to the students and faculty. Electronic networks, including the Internet are a part of the instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

In order for the school to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students utilizing school-provided Internet access are responsible for good behavior on-line.

The same general rules for behavior apply to students' use of school-provided computer systems. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the teachers and other staff will make reasonable efforts to supervise use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Curriculum

The use of the school's electronic networks shall be consistent with the curriculum adopted by the school as well as the varied instructional needs, learning styles, abilities, and developmental

levels of the student and shall comply with the selection criteria for instructional material and library-media center materials. Staff members may, consistent with the school's educational goals, use the Internet throughout the curriculum.

The school's electronic network is part of the curriculum and is not a public form for general use.

Acceptable Uses

1. Educational Purposes Only All use of the school's electronic network must be (1) in support of education and/or research, and be in furtherance of the school's stated educational goals or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the school's electronic network computers. The school reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage.

2. Unacceptable Uses of Network The following are considered unacceptable uses and constitute a violation of this policy:

A. Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages offering for sale or use any substance whose possession or use is prohibited by the school's student discipline policy; viewing, transmitting, or downloading pornographic material or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.

B. Uses that cause harm to others or damage to their property, including but not limited to, engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information.

C. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.

D. Uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. Students and others should not give information to others, including credit card numbers and social security numbers.

E. Students are prohibited from using e-mail; this includes school e-mail accessed through a web browser. E-mail access may be given to students on a case-by-case basis (e.g., foreign exchange students keeping in contact with home). Students are prohibited from joining chat rooms, unless it is a teacher-sponsored activity.

Internet Safety

Each school computer with Internet access shall have a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act.

The school will also monitor the online activities of students, through direct

observation and/or technological means, to ensure that students are not accessing such depictions or other material that is inappropriate for minors.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file or other visual depiction that:

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Filtering should only be viewed as one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Filtering should be used in conjunction with:

- Educating students to be "net-smart";
 - Using recognized Internet gateways as a searching tool and/or home page for students, in order to facilitate access to appropriate material;
 - Using "Acceptable Use Agreements";
- Using behavior management practices for which Internet access privileges can be earned or lost~ and
 - Appropriate supervision.

Building principals shall monitor student Internet access.

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student him/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Internet Access Conduct Agreements

Each student and his/her parent(s)/legal guardian(s) will be required to sign and return to the school at the beginning of each school year the Internet Access Conduct Agreement prior to having access to the school's computer system and/or Internet service.

Warranties/Indemnification

The school makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The school is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. The school will not be responsible for any unauthorized charges or fees resulting from access to the Internet and any user is fully responsible to the school and shall indemnify and hold the school, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such users'

access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchase of goods or services by the user. The user, or, if the user is a minor, the user's parent(s) legal guardian(s) agrees to cooperate with the school in the event an investigation of a user's use of his/her access to its computer network and the Internet.

Violations

If any user violates this policy, the student's access will be denied, if not already provided, or withdrawn and he/she may be subject to additional disciplinary action. The building principal will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke or suspend access at any time with his/her/their decision being final.

INTERNET ACCESS CONDUCT AGREEMENT

Every student, regardless of age, must read and sign below:

I have read, understand, and agree to abide by the terms of the school's policy regarding Access to Electronic Information, Services, and Networks. Should I commit any violation or in any way misuse my access to the school's computer network and/or the Internet, I understand and agree that my access privilege may be revoked and school disciplinary action may be taken against me.

User's Name (Print): _____ Home Phone:

—

User's Signature:

Date:

Address:

Status: Student

Staff

Patron

I am 18 or older

I am under 18

. If I am signing this policy when I am under 18, I understand that when I turn 18, this policy will continue to be in full force and effect and agree to abide by this policy.

Parent or Legal Guardian, (If applicant is under 18 years of age, a parent/legal guardian must also read and sign this agreement.) As the parent or legal guardian of the above named student, I have read, understand and agree that my child shall comply with the terms of the school's policy regarding School-Provided access to Electronic Information, Services and Networks for the student's access to the school's computer network and/or the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's responsibility for abiding by the policy. I am, therefore, signing this Agreement and agree to indemnify and hold harmless the school, the Trustees, Administrators, teachers, and other staff against all claims, damages, losses, and costs, of whatever kind that may result from my child's use of his /her access to such networks or his/her violation of the school's policy. Further, I accept full responsibility for supervision of my child's use of his/her access account if and when such access is not in the school setting. I hereby give my child permission to use the building-approved account to access the school's computer network and the Internet.

Parent/Legal Guardian (Print):

—

Signature:

Address: _____

Home phone: _____

Date: