Green Bay Area Catholic Education
Student Technology Acceptable Use Policy

Green Bay Area Catholic Education (GRACE) provides students with an opportunity to access computers, the network and the Internet. A goal in providing these services to students is to promote learning by facilitating resource sharing, innovation and communication skills. In addition, this provides the opportunity to teach responsible and ethical use of technology in their daily lives.

GRACE complies with the Children's Internet Protection Act (CIPA) which is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

The policy regarding the use of technology and the Internet at GRACE.

- GRACE technology includes, but is not limited to, computers, the system's computer network including servers and wireless computer networking technology (Wi-Fi), the Internet, email, USB drives, chromebooks, tablet computers, smartphones and smart devices, telephones, cellular telephones, MP3 players, wearable technology, any wireless communication device and/or future technological innovations.

All school computer network accounts and student's personal electronic devices must be used in support of education and research and be consistent with the educational mission and goals of GRACE.

- Transmission of any material in violation of any state or federal regulation is prohibited.
- This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret.
- Use of the school computer network account for commercial activity, for product advertisement or for political lobbying is prohibited.

G Suite for Education (formerly Google Apps for Education) is administered by the GRACE technology coordinators where by default access of Google APPs are denied, unless explicitly granted. Students have parent/guardian permission to access GRACE approved apps with approval/signature of this GRACE Student Technology Acceptable Use Policy.

Students and school personnel receive a password to access the school network. The users keep all passwords confidential. User passwords are changed if someone else may know it or the account has been abused by others.

Not all information on the Internet is of educational value in a school setting. While software is implemented to filter Internet content, there is still potential for students to access inappropriate material.Use of the Internet by GRACE students will be supervised by adults at all times. Intentionally accessing any inappropriate sites on the Internet is strictly forbidden.

Rules for Internet Use at GRACE

- I will not download any files from the Internet unless I have permission.
- I will obey and uphold the copyright laws (plagiarism) and other applicable laws and regulations.
- I must always document sources, in both formal and informal communications (reports, writings & email).
- I will not post any communications in public forums unless I have permission.
- I will not send e-mail unless I have permission.
- I will not access non-educational sites.
- I will not play games or access game websites unless approved, at that time, by the teacher.
- I will not use inappropriate language in any Internet communications.
- I will not intentionally search for, view and/or distribute inappropriate materials.
- I will not give personal information about myself or others on the Internet.
- I will not post anonymous or false information on the Internet.
- I will not harass others on the Internet.

The use of social networking, blogs, wikis, podcasts and other internet tools are considered an extension of the classroom as directed by the teacher. Students using web tools are expected to act safely by keeping ALL personal information out of their posts. Students using these tools are expected to keep their username or password private with the exception of their teachers and parents. Students who do not abide by these conditions may lose their opportunity to participate in the activity and/or be subject to consequences as directed by this policy.

The school network and equipment may not be used to harass, tease, intimidate, threaten or terrorize others. Cyberbullying is the posting of inappropriate and hurtful email or text messages, digital pictures or web site postings, including blogs, social networking sites and other web tools. Students and school personnel, who believe they are a victim of cyberbullying, should notify a parent/guardian and the school principal.

We believe that providing use of personal electronic devices will enhance the educational experience by expanding access to the resources provided by the Internet and these personal electronic devices (cell phones, laptop computers, electronic notebooks, tablets, e-readers, etc). The use of the privately owned electronic device is solely limited to support and enhance instructional activities currently occurring in the classroom environment.

Green Bay Area Catholic Education (GRACE) will allow personal electronic devices/ wearable technology with these considerations:

- Devices may be used in classrooms and study halls with the permission of the classroom teacher and for educational purposes; any other use is prohibited while on the school premises.
- Use of personal electronic devices is prohibited in locker rooms, dressing rooms, bathrooms, or other locations that are private in nature.
- Possession of these devices in school is at the student's own risk. Sharing of personal devices between students is highly discouraged.
- Students themselves are solely responsible for any loss, damage or liability related to their devices being used by them or others.
- The school is in no way liable for loss, damage or misuse of the devices or any costs including, but not limited to text minutes, data plans and other costs associated with the use of the personal electronic device.
- Any costs related to the use of such devices in school during instruction are the responsibility of the student and/or the student's family.
- No student shall establish a wireless ad-hoc or peer-to-peer network using their electronic device or any other wireless device while on school grounds. This includes, but is not limited to using a privately owned electronic device such as a cabled or wireless hotspot.
- No one is allowed to connect a privately owned electronic device in the network by an Ethernet cable plugged into a school data jack. Violation will result in disciplinary action and revocation of access to the network.
- Any student refusal to follow staff instructions related to the use of personal electronic devices will be dealt with according to this technology policy (see below).
- Where wireless network (WIFI) connection is available for student use, it is intended to allow student access to the internet for educational purposes. Students may not deliberately use the network in such a way that would disrupt network use for other users (i.e. downloads or use streaming video/music).

The use of technology and the Internet at a GRACE school is a privilege, not a right, and any student abusing that privilege will no longer be allowed the use of technology and the Internet at GRACE. Any actions related to or in support of illegal activities will be referred to local authorities for further legal action.

The technology coordinator, faculty and administration will judge what is offensive and an inappropriate use of technology and Internet. A student who is found to be using the technology and the Internet inappropriately will not be given a warning. The first offense will result in loss of technology and Internet privileges for duration of time determined by the technology coordinator and principal (maximum penalty – loss of technology and Internet privileges for the balance of the school year). If the infraction involves a student's personal electronic device, it will be confiscated immediately. The student's parent(s) may pick up the confiscated device in the school office.

All GRACE school students and parent(s)/guardian(s) must read the rules and policies regarding the use of the Internet at GRACE. Before network and Internet access is allowed, the students and parent(s)/guardian(s) must sign the Technology Acceptable Use Policy (AUP) annually stating they have read the policy and will abide by the rules.

SAFE ENVIRONMENT SOCIAL COMMUNICATIONS POLICY FOR THE DIOCESE OF GREEN BAY

Social networks and other digital communication offer individuals, groups and the Catholic Church an opportunity to connect in positive ways. We are able to encourage one another, strengthen community ties and boldly proclaim the Gospel of Jesus Christ.

While communication has technically advanced, it is at its core a human interaction. This *Safe Environment Social Communications Policy* creates clear standards and expectations for online and digital communication to protect children, youth and individuals at risk in virtual spaces. A Diocesan location or system may adopt a local practice that is stricter than this policy but may not adopt a practice that fails to meet the standards and expectations that follow.

Adherence to Diocesan Codes of Conduct

All communication of clergy and employees (referred to as "ministry representatives" in this document) of the Diocese of Green Bay with non-related minors and individuals at risk should conform to "*Our Promise to Protect" - Safe Environment Policy, Diocese of Green Bay* (http://www.gbdioc.org/images/stories/Protecting/pdf/Our_Promise_to_Protect_2012.pdf).

Ministry representatives should always remember that they are representatives of their parish, school or Catholic organization, and should conduct themselves accordingly, sharing a positive, joyful witness to the Gospel with others at all times.

Mandatory reporting

Ministry representatives must immediately report any form of social communication they receive which indicates existing or imminent harm or danger of sexual abuse of a minor to civil authorities. The content of the communication must also be reported to parish leadership, and the Safe Environment Coordinator (920-272-8174) in collaboration for the safety of the individual.

Parents as primary catechists and decision makers

Parents are the primary catechists and role models of discipleship to their children. All ministry representatives have a responsibility to respect the wishes and stated desire of parents with regard to their child's level of participation in the use of social media or any form of digital communication and the parent's right to be aware of the content of non-public communications between ministry representatives and their children.

A parent or guardian must complete the ***Parental/Guardian Statement of Intent*** before any ministry representative may engage in any electronic communication with any unrelated minor or individual at risk, with whom they have any connection because of their ministry. The signed ***Parental/Guardian Statement of Intent*** is kept on file at the local level, and it should be refreshed annually. No ministry representative may engage in any non-public electronic communication (any digital communication to which a parent or guardian does not have direct and immediate access) with any unrelated minor or individual at risk without a parent or guardian having granted permission (selecting "Yes, I authorize") to do so in the ***Parental/Guardian Statement of Intent.***

Guidelines for use of written words, photos, videos and audio recordings

Clergy, employees, and volunteers must obtain parental or guardian permission to photograph, videotape or otherwise record, copy or distribute any personally identifiable information - including, but not limited to, a minor's full name, photograph, video recording, audio recording, home address, email, telephone number, creative work or any other form of content that would allow someone to identify or contact that minor or individual at risk.

A standard of transparency

Ministry representatives are always witnesses and disciples of Jesus Christ. Therefore, complete transparency is imperative and necessary regarding the content of all digital communication with unrelated minors or individuals at risk.

All ministry representatives must agree to all communication between themselves and any unrelated minor or individual at risk is open to review, and each parish, school or organization must retain consent for this on their premises. This written consent is included as part of the acknowledgement and agreement form for this Policy. Ministry representatives will refrain from using any platform where a record or archive of communication cannot be obtained.

Ministry representatives must always be able to be identified personally in any web, social networks or any other digital profile by their common name or photo. Aliases are not to be used. If you are an employee, an official email account connected to the parish, school, ministry or diocese must be used for all email communication with unrelated minors and individuals at risk. Whenever practical, an official parish, school, ministry or diocese platform should be used for other types of social media communication as well.

Ministry representatives must maintain appropriate boundaries and should use language in their posts that clearly reinforces and identifies their role or affiliation with that ministry, when promoting or discussing ministry events.

Parents or guardians have the right to be made aware of and to request to review non-public social communication between their child or individual at risk, and ministry representatives in its various forms. In exceptional situations when a parent or guardian is not made aware of the content of a non-public social communication, the ministry representative must share that communication with their Supervisor or another ministry representative or another Virtus trained, background-checked adult if the Supervisor is unavailable. It is up to the individual parish, school or organization to determine the form and standards in which this is made available to individuals and how it is retained. Informing parents or guardians is not required for non-private communications such as those sent to youth groups regarding meeting locations or times or other administrative matters.

Accountability

For the protection of all individuals, it is *highly recommended* that ministry representatives follow a *TWO PLUS ONE Policy* for digital communication responding to unrelated minors and individuals at risk. The TWO PLUS ONE standard follows that whenever a ministry individual has the chance to invite another VIRTUS-trained, background-checked adult into the communication, they should do so. This standard fosters safe environments by providing transparency, accountability and a second, checked adult presence when digital communication takes place.

Any parish, school or organization that creates an official ministry page, social media outlet or other digital presence is required to have at least one *paid staff member* maintaining administrator-level privileges to each web-based or social media outlet. This staff member should be assigned as the designated “primary contact” for the outlet, and this information made available to parents.

Questions

Any questions about this policy may be directed to the Office of Safe Environment at 920-272-8174.

Rev. August 2017