**INTRODUCTION**

Access to technology resources is provided to members of the GCC community strictly in support of activities related to GCC and classroom learning. This Policy applies to both students and employees , Users, who have access to diocesan equipment, network services, and instructional resources on school property, at school-related off campus activities, and at off-campus locations, such as at home for virtual classes and preparing homework. Technology resources that are covered by this policy include, but are not limited to, computers, servers, printers, video and audio devices, cameras, software, infrastructure equipment, cloud services (including cloud sharing and cloud storage), storage devices, copiers, telephones, cell phones, eBook readers, iPads, tablets, web-based instructional tools, applications (Apps), wearable technology, non-fungible tokens (NFTs), drones, 3D printers, virtual reality and augmented reality equipment and services, location devices, biometric devices, artificial intelligence (AI) tools, such as chatbots, and other resources.

Users must agree to act in a responsible manner and in compliance with this Acceptable Use Policy, as well as other diocesan policies. Users are responsible for their conduct, actions, and communications when using personal and/or school technology resources. They are responsible for the appropriateness and content of material they store, transmit, or publish. General school rules for conduct and communication apply in addition to the requirements of this Policy and other relevant diocesan policies.

This Policy, and any subsequent policies, are designed to make technology available to the GCC community and promote the responsible and safe use of resources. Cooperation and adherence to this Policy is a condition of access to the aforementioned resources. Violation of this Acceptable Use Policywill result in disciplinary action, which may include removal of access or other applicable consequences up to and including expulsion or dismissal, as appropriate. A violation may have significant legal and/or financial consequences.

**ACCEPTABLE AND UNACCEPTABLE USE**

The Internet offers the capability for Users to access and share information on a global scale. The scholarly use of the Internet can provide our Users with a world-wide, diverse array of resources.

However, while the Internet is an exciting resource tool, Users must be aware that there are services and information available through the Internet that could be offensive and unsuitable for certain groups of Users.

Users must observe the following practices and precautions to help ensure that the use of technology is a safe, productive, and educationally rewarding experience:

1. Users will be given permission to access the Internet for school personnel sponsored activities only. There are many valuable educational resources via the Internet. Only access to discussion groups on social media sites will be permitted through secured sites sponsored by school personnel and involving authorized participants only. All other access to such sites is strictly forbidden.

2. When the Internet is used in real time and during school hours, content filtering and blocking software will be utilized for blocking subjects, words or images that are deemed inappropriate.

3. Users will be instructed in the proper use of the Internet and practices that will help limit inadvertent access to inappropriate information and will help them develop skills in evaluating sources of information, whether online, on TV or in hardcopy. Because Users can link to sites other than those permitted, and because school personnel cannot be expected to monitor Users’ use of the Internet at every moment, individuals must assume responsibility for their own appropriate use of the Internet according to this Policy.

4. Users must consent to the appropriate use of **cloud computing services, including cloud sharing and storage,** as follows.

4.1 Users may not place, transfer, transmit, or store diocesan student, employee, and other diocese confidential, sensitive, and personally identifiable information (PII) beyond the diocese authorized cloud services. Public or consumer-based cloud products and/or services may not be used without the consent of the diocese. As an example, teachers or administrators working on any student assessment and storing it in their personal cloud service account such as DropBox , Vimeo, iCloud or Google Workspace, is not authorized by the diocese.
4.2  Users’ confidential, sensitive, and PII must be encrypted with diocese authorized encryption during use. Users must use the authorized encryption and, if appropriate, decryption software/service. Use of unauthorized encryption, decryption, and anonymizers are prohibited.

4.3 Only cloud services supported by the diocese Office of Information Technologies and approved via the Technology Request approval process may be used by Users. Other Users may not agree to contractual terms that subject the diocese to cloud agreements, terms, and conditions. For example, a teacher may not click and agree to download an App for instructional material to use with students without the App being approved by and/or listed on the diocese approved Apps list.
4.4 The diocese may not agree to any terms (e.g., in a website privacy policy or terms of use, or in any other agreement) in any manner to give cloud providers or any online service, student confidential, sensitive, and PII for the provider’s commercial, behavioral advertising, and/or student User profile product development and marketing.

Users agree to the following practices to ensure **personal safety and well-being**:

1. User agrees to use only their school provided e-mail account for all academic and school affiliated activities to ensure successful transmission of messages to and from faculty and administration and to better ensure the security of email from viruses and malware.
2. While using school provisioned resources, the User agrees not to transmit PII (name, age, gender, social security number, address, phone number, credit/debit card information and the like) of himself, herself, or other person. If this is necessary, the User must work with administration in calling the Help Desk to receive instruction on encrypting such communication.
3. Student Users must not agree to meet with someone they have met online without their parents' full approval and participation.

User agrees to notify school personnel immediately if he or she is asked for personal information, to view inappropriate materials, or in any other way feels violated, harassed, uncomfortable, or accosted through the use of the school's technology resources.

Users agree to the following statements regarding **illegal/unauthorized activities and system security**:

1. User agrees to access only the Internet and network resources, software and/or hardware provided expressly by the school for educational purposes.
2. User agrees to follow the procedures and best practices recommended by school personnel or system administrator. These procedures and practices must address respect for the resource limits of the school, personal safety issues, and/or access to appropriate materials.
3. User agrees not to use the network in such a way that would disrupt the use of the network for others. Disruptions include, but are not limited to, propagation of viruses and other malware; use of the network to make unauthorized entry to any other machine accessible via the network; posting information that if acted upon could cause damage, danger, or school or system disruption; attempting to log in through another person's account; and sending unnecessary messages to a large number of people (spamming).
4. User agrees not to tamper with or vandalize the technology property of the school, off-campus location, or other User including, equipment; cabling and other infrastructure; any security system that protects the schools’ and other locations’ computer resources; and facilities and data. Vandalism is defined as any malicious attempt to harm or destroy data or equipment of another User, the school, the school network, or any other network.
5. User agrees to respect another's email by not tampering with, interfering with, or intercepting electronic communications. Numerous laws prevent such tampering, and the interference and interception, some of which could result in civil or criminal actions.
6. User agrees not to use the schools’ resources to gain unauthorized access to another computer network (for example, hacking and unauthorized tracking).
7. User agrees not to use or respond to inappropriate, obscene, profane, rude, inflammatory, threatening, or disrespectful language.
8. User agrees not to post false information or engage in personal, prejudicial, or discriminatory attacks.
9. User agrees to adhere to the Diocese of Greensburg Web Content Policy which states that the school affiliated domain names (e.g. domain names representing the school in any manner - sports, club activities, etc.) must be owned by the school.
10. User agrees to at no time unlawfully harass, intimidate, haze, or bully (which includes cyberbully) another person through the use of any school resources and/or personal communication devices. See Diocese Policy Health & Safety section 619, Prohibiting Harassment, Intimidation, Hazing, or Bullying (also reference your Student Handbook). The User agrees to stop immediately any and all conduct that is construed by another as unwelcome.
11. The diocese supports the Children’s Internet Protection Act (CIPA) requirements by actively using content filtering and the iSafe Internet Safety program at all of our schools. Users must comply with the program.
12. User agrees not to access, possess, transmit, re-transmit or respond to any information containing sexually oriented material, other than diocesan approved curricula.
13. User agrees not to use technology resources to engage in any illegal, criminal activity or any conduct which is morally inappropriate and/or violates Catholic teachings. The school will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities.
14. User agrees not to use the school and school affiliated network and devices for commercial sales, multilevel marketing, gambling, sweepstakes, chain letters, or similar unauthorized purposes.
15. Online games may only be accessed for educational purposes with the consent of the student’s administrator or teacher.
16. User agrees to not access the school and school affiliated network for political lobbying, although it may be used, with the permission of the principal, to communicate with elected representatives to express opinions on political issues.
17. User agrees not to plagiarize. Plagiarism is defined as taking the idea or writing of others and presenting them as one's own.
18. User agrees to respect the right of intellectual property of other people and to respect all copyright laws. Students agree that if they are unsure whether copyright law is being respected, they will take their question immediately to a faculty member.
19. The use of diocese authorized blogs, vlogs, wikis, podcasts, cloud storage (as it relates to sharing), crowdsourcing, or other social interactive web tools to name only a few, extend beyond the classroom. Therefore, speech that is considered inappropriate in the educational and instructional setting, such as unlawful harassment, intimidation, hazing, and bullying (including cyberbullying) are also inappropriate for use in the above media supported by the diocese listed in this section. This includes but is not limited to profanity, racist, sexist, or discriminatory remarks. (See #10 above.)
20. Students should only create a class blog, vlog, wiki, or other media for educational purposes and with permission of school personnel. Student profiles are not permitted to be used to create personal blogs, vlogs, or wikis. Students are not permitted to link to websites from your blog, vlog, blog/vlog comment, or wiki without reading the entire article to make sure it is appropriate for a school setting.
21. The use of social media sites by Users (e.g. Facebook, Instagram, etc.) for personal reasons are not allowed during school hours. Please reference the diocesan Social Media Policy.

***Use of Technology:***

**3D Printers**

The diocese provides Users 3D printers, scanners, and related equipment (“3-D printers”) to use when there is a diocesan instructional or administrative reason for their use. The 3-D printers may be used only for these purposes. Approval by a teacher or administrator is required for the User to operate a 3D printer. If approved, the person approving such use must then supervise the User’s’ use.

Use of 3D printers must comply with diocese policies and other legal requirements. For example, no created object: (i) may violate local, state or federal law; (ii) may involve inappropriate matter (as defined by the diocese in its policies, regulations, and other governance sources); (iii) may be unsafe, harmful, dangerous, or may pose an immediate threat to the well-being of others (for example, knives, guns, or lethal weapons); and (iv) may violate the intellectual property rights (copyright, patent, trade secret, trademark) of the owner.

Users must understand the risks associated with 3D printing, including the physical damage or harm when they are transporting and using a 3D printer, the malfunctions of a 3D printer, or the defects in the objects. The diocese will not guarantee the quality or stability or the confidentiality of the designs or be liable for any object created with the use of the 3D printers, including harm or injury incurred as a result of the use of the equipment.

The school administration, and/or designee, is authorized to prepare and enforce administrative regulations and/or rules to carry out the use of 3D printers.

**Wearable Technology**

The diocese recognizes that Users may be wearing personal computing devices for personal or efficiency reasons. These wearables are part of the Internet of Things (IoT) that include fitness and health trackers, ready-reference devices (provides access to the world of online information), and history-recording devices (records the wearers’ and possibly others’ experiences).

The IoT are items (everyday objects that have network connectivity, allowing them to send and receive data), including vehicles with smart technology, and wearable smart devices that can be worn by a person, either as an accessory or as part of material used in the clothing, and is able to be connected to the Internet, enabling data to be exchanged between a network and the device (for example, smart watches, smart clothing, fitness trackers, football helmets, and smart jewelry).

If students are using the diocese’s WiFi or Internet service, the students, employees, or guests have no expectation of privacy in anything they create, store, send, receive, or display on or over the diocese’s computers, servers, networks, printers, video and audio devices, cameras, software, infrastructure equipment, copiers, and electronic communication devices (e.g., cell phones, iPads, telephones, eBook readers, tablets, and other electronic resources. They have no expectation of privacy in their personal files or any of their use of the diocese’s computer systems. The diocese reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any or all computer systems’ use and to monitor and allocate cloud and/or fileserver space. The diocese does not require students to wear or use diocese wearable technology. Therefore, the diocese does not attempt to collect the information and data through diocese wearables.

If a student’s wearable collects personal information from other individuals, the diocese is not liable for the student’s collection, use, storage, or other action(s) with respect to the information or data they collect.

**One-to-One Device Usage**:

* Students agree to the practices outlined in the Student Equipment Receipt and Use Agreement that was signed when Users received their device.
* Non-functioning devices are not an excuse for lack of preparation for class, participation in class, or failure to complete assigned work.
* Students must follow the Help Desk policy for guidance on how to receive technical help and support on their school provided electronic devices. Help Desk support is limited to the schools’ owned devices; no assistance will be given on personally owned devices.

**Privileges and Enforcement:**

The use of digital networks and technology is a privilege, not a right. Access is given to Users who agree to the terms of this Acceptable Use Policy and other diocese policies. Inappropriate use or a violation of this Policy result in the User's access privilege being suspended, denied, or revoked. Misuse may also subject the User to further disciplinary action as deemed necessary by the administration, as well as action taken by the terms of use and privacy policies of third-party websites and other media. Any violation of federal, state, or local laws will be reported to the appropriate agencies. The school maintains the right to confiscate and lawfully search any personal electronic devices found on school premise or used during school hours.

The law and the diocese do not recognize an absolute right to freedom of speech when using the school’s technology resources and/or personal technology devices, which are viewed by the administration as a limited educational forum. All e-mail and other media communications through the diocese services and equipment remain diocesan property. The diocese reserves the right for its authorized representatives, as specified, and with written approval from the superintendent to access, use, and disclose the contents of electronic mail files for legitimate educational and business purposes (including responding to legal processes in any matter consistent with state and federal law) without the permission of the User. It is a violation of this policy for any User, of the diocese, or school or parish within the diocese, including management, to access the mail files of Users to satisfy personal curiosity without a legitimate business need.

**Privacy:**

There is no absolute right to privacy when using the school’s technology resources. Network administrators may review files and communications to maintain system integrity and ensure that Users are using the system responsibly if requested by the building principal or superintendent. School personnel will have the right to review any and all material saved, transmitted, accessed, or momentarily in use by the Users in accord with the policy set by the school’s administration. Users should not expect that files will be private (see Introduction, paragraphs 2 and 3).

**Liability:**

GCC and its employees will not be held responsible for the actions of a User who is in violation of any of the terms of this Policy. This responsibility is extended to, but not limited to: loss or unavailability of data or interruptions of service, violations of copyright and other intellectual property restrictions, the accuracy or quality of information obtained through the school's system, or any liability, damages, or financial obligations arising through the unauthorized use of the school's and/or personal technology resources.

**Warranties:**

GCC and diocese make no warranties of any kind, whether expressed or implied, for the service being providing.

* The school and diocese will not be responsible for the accuracy, quality, or usefulness of information obtained through network connections.
* The school and diocese will not be responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties.
* The school and diocese will limit individual User network storage/disk space specific to the needs/responsibilities of the User and will not be liable for use beyond this limitation.
* The school and the diocese will not be responsible for the contents of any website bearing their name(s) unless the web page has been authorized by the administration of the school and/or the diocese.
* The school and diocese administration reserves the right to establish rules and regulations regarding the use of the system.

**GCC TECHNOLOGY RESOURCE AND COMMUNICATION SYSTEM**

# PARENT/GUARDIAN PERMISSION TO ACTIVATE USER PRIVILEGES

# I certify that I have read the terms and conditions in the GCC Acceptable Use Policy and discussed them with my child. I understand that access to the Internet, technology and communications systems are designed for educational, security, and safety purposes and that my child has agreed to abide by the school’s usage rules. I understand that my child has responsibility for his or her actions in regard to the use of technology resources and recognize my responsibility for governing and guiding access and use both inside and outside of the school setting. I also understand that the consequences, as stated in the policy, for inappropriate actions or conduct. I recognize that it is impossible for the school to restrict access to all controversial materials and I will not hold the school, diocese or their personnel responsible for material acquired or viewed through technology resources. I hereby give my permission to activate any school technology privileges for my child.

I acknowledge that the diocese has consented to the collection of student data, for academic reasons, on my behalf on all websites and online services that are accessible via the official school and diocesan websites.

**PARENT / GUARDIAN PERMISSION FOR ONLINE PUBLISHING OF STUDENT WORK AND STUDENT PHOTOGRAPH AND FOR PUBLISHING OF STUDENT’S PHOTOGRAPH AND SCHOOL WORK IN THE CATHOLIC ACCENT AND ON THE SCHOOL AND DIOCESAN WEBSITES AND SOCIAL MEDIA OUTLETS**

I understand that my child's photograph and samples of my child's schoolwork may be published in The Catholic Accent, on the school and/or diocesan websites or social media outlets. I further understand that the work will appear with a copyright notice prohibiting the copying of such work without express written permission. In the event a request is made for such permission, those requests will be forwarded to me as parent/guardian. I understand the school and the faculty will be the contacts responsible for the work published and that the school’s address, telephone, and email addresses appear on the school’s website. I understand that I can request that my child's individual picture or school work not be published on the school’s website or social media outlets. This is not inclusive of any group, class, or school production photos utilized on the website or by members of the media.

I understand that if at any time I *do not* wish to have my child's individual photo and/or samples of my child's school work published in The Catholic Accent, diocesan or school websites or social media outlets, I will submit written notification, including the date, child's name, and grade to the school principal.

**STUDENT PERMISSION TO ACTIVATE USER PRIVILEGES**

I certify that I have read the terms and conditions in the GCC Acceptable Use Policy and discuss them with my child.

I understand that access to the Internet, technology and communications systems are designed for educational, security, and safety purposes and that I have agreed to abide by the school’s usage rules.

I have received, read, and understand the Student Acceptable Use Policy, and will comply with it. Someone from the School has also reviewed it with me and my parents have reviewed it with me. In addition, I have been given the opportunity to obtain information from the diocese and my parent(s) about anything I do not understand, and I have received the information I requested.  If I have further questions, I will ask the school principal and my parents. If I need a copy of the Policy, I understand that I can access it on the diocese’s website. Additionally, I understand that if I violate the Policy or other diocesan policies, regulations, rules, and procedures I am subject to the school’s and diocese’s discipline, and could be subject to Internet Service Provider’s, website’s, and app’s rules, as well as local, state and federal laws and procedures.

I understand that protecting network, email and cloud computing passwords is critical to security and my student privacy. I accept responsibility for protecting my passwords at all times, regardless of the location from which I access these systems. I understand that I am not to share my password with anyone, including my teacher or school principal. I will not allow others to access systems through my account. I understand that failure to protect my passwords and accounts can result in loss of access to systems from both inside and outside of the school building as well as further disciplinary action.

I also understand the consequences, as stated in the policy, for inappropriate actions or conduct.

**STUDENT PERMISSION FOR ONLINE PUBLISHING OF STUDENT WORK AND STUDENT PHOTOGRAPH**

I understand that my photograph and samples of my school work may be chosen to be published in the Catholic Accent, on the school and/or diocesan websites or social media outlets.

**Internet and Email Form of Understanding
Online Publishing of Faculty/Staff Work Permission Form**

**Faculty / Staff Form of Understanding
For Internet Access and Use of Electronic Mail**

I have read and understand the information about appropriate use of the computer network with Internet access and electronic mail communication at GCC. I understand that this form will be kept on file at school. I understand the risks and benefits of Internet access. I understand that I have a responsibility to prepare, evaluate, and preview Internet sites and activities that I recommend to students or use within my classroom. I appreciate the unpredictability of Internet use and realize I must outline/emphasize/enforce proper procedures for Internet searches and accessing Internet sites through URL addresses. I also understand the rules governing my use as well as students’ use of electronic mail and so my role in reading the messages to be sent and those received. I accept my responsibility for governing and guiding Internet access.

I understand that protecting network, email, cloud computing and student information system (SIS) passwords is critical to system security and student privacy. I accept responsibility for protecting my passwords at all times, regardless of the location from which I access these systems. I understand that I am not to share my password with anyone, including my supervisor. I will not allow others to access systems through my account. I understand that failure to protect my passwords and accounts can result in loss of access to systems from outside of the school building as well as further disciplinary action.

**Faculty / Staff Permission Form**

**For Online Publishing of Work**

I understand that my work may be published on the Internet. I further understand that the work will appear with a copyright notice prohibiting the copying of such work without express written permission. In the event anyone requests such permission, those requests will be forwarded to me. No home address or telephone numbers will appear with such work. I understand the school and other faculty will be the contacts for the work published and that the school’s address, telephone, and email addresses appear on the school’s website.

I grant permission for the publishing of my work on the Internet.