Acceptable Use Policy Agreement For School Name

Last updated August 2018 (for reference only)

INTRODUCTION

Access to technology resources is provided to members of the school community strictly in support of activities related to school and classroom learning. Access to equipment and network services is given to those members who agree to act in a responsible manner and in compliance with this Acceptable Use Policy Agreement. Students and staff 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 Diocese policies. Technology resources that are covered by this agreement include, but are not limited to, computers, servers, printers, video and audio devices, cameras, software, infrastructure eq., copiers, telephones, cell phones, eBook readers, iPads, tablets, apps, wearable technology, drones, 3D printers, virtual reality and augmented reality equipment and services, location devices, biometrics, and other electronic resources.

This Policy, and any subsequent policies, is designed to make technology available to the school 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 Policy will result in disciplinary action, which may include removal of access or other applicable consequences, and may have significant legal and/or financial consequences.

ACCEPTABLE AND UNACCEPTABLE USE

The Internet offers the capability for students and staff to access and share information on a global scale. The scholarly use of the Internet can provide our students and staff 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 will observe the following practices and precautions to help ensure that the use of technology is a safe, productive, and educationally rewarding experience:

1. In the school setting, students 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 or social networking sites will be 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. Students 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 on-line, on TV or in hardcopy. Because students can link to sites other than those suggested and because school personnel cannot be expected to monitor student 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 and storage as follows.

4.1 Employees and guests may not place, transfer, transmit, and store Diocesan Student Confidential, Sensitive, and Personally Identifiable Data and/or Information beyond the Diocese authorized cloud service in public or in consumer-based cloud products and/or services without the consent of the Diocese. As an example, teachers working on any student assessment and storing it in their personal cloud service account such as DropBox, is not authorized by the Diocese.
4.2 Diocesan contracted and secured cloud services provided by Microsoft Office 365 (O365) are the only authorized cloud services for students and employees to use. The use of any other cloud service (for example, G Suite for Education) for Diocese data/information must be approved in writing by the Superintendent and Director of Information Technologies.
4.3 Diocese Student Confidential, Sensitive, and Personally Identifiable Data and Information may be required to be encrypted with Diocese authorized encryption during use. If so, employees and guests must use the authorized encryption and, if appropriate, decryption software/service. Use of unauthorized encryption, decryption, and anonymizers are prohibited.
4.4 Only authorized Diocese administrators using authorized Diocese procedures may enter into cloud computing, cloud services, and/or cloud storage contracts. Other employees, guests, and students 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 their building administrator's approval.
4.5 The Diocese may not give cloud providers student Confidential, Sensitive, and Personally Identifiable Data and Information for the provider's commercial behavioral advertising and student user profile product development and marketing.

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

1. The student 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. At school, the user agrees never to transmit personal information (name, age, gender, photo, address, phone number, credit/debit card information and the like) of himself or herself as well as that of any other person. If this is necessary, the student must work with administration in calling the Help Desk to receive instruction on encrypting such communication.
3. The student agrees never to arrange for a meeting with any person at any time using the school's technology resources. Student users will not agree to meet with someone they have met online without their parents' full approval and participation.
4. The student agrees to notify school personnel immediately if he or she is asked for personal information, views 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. The user agrees to access only the Internet and network resources, software and/or hardware provided expressly by the school for educational purposes.
2. The user agrees not to access Diocese and/or ***personal*** electronic communication devices, electronic networks, wireless capable devices such as iPads, tablets, mobile phones, laptops, and other similar items, during school hours unless authorized by faculty, according to schools' administrative guidelines.
3. The user agrees to follow the procedures and best practices recommended by school personnel or system administrator. These procedures and practices may address respect for the resource limits of the school, personal safety issues, and/or access to appropriate materials.
4. The user agrees never 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).

5. The user agrees never to tamper with or vandalize the property of the school or other user including: equipment; cabling and other infrastructure; any security system that protects the school's computer resources; 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.
6. The user agrees to respect another's email by never tampering with, interfering with, or intercepting electronic communications. Numerous laws prevent such tampering, interference and interception, some of which could result in civil or criminal actions.
7. The user agrees never to use the school's computer resources to gain unauthorized access to another computer network (hacking).
8. The user agrees never to transmit (download or upload) any computer file, application, or other computer resource to or from the school's computer network without approval.
9. The user agrees never to use or respond to inappropriate, obscene, profane, rude, inflammatory, threatening, or disrespectful language.
10. The user agrees never to post false information or engage in personal, prejudicial, or discriminatory attacks.
11. Students, faculty, and all school personnel agree 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.
12. The 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 4445, Prohibiting Harassment, Intimidation, Hazing, or Bullying (Appendix B of Student Handbook). The user agrees to stop immediately any and all conduct that is construed by another as unwelcome.
13. We support the Children’s Internet Protection Act (CIPA) requirements by actively using content filtering and the iSafe Internet Safety program at all of our schools. Employees and students must comply with the program.
14. The user agrees never to access, possess, transmit, retransmit or respond to material which promotes violence or discrimination or advocates destruction of property.
15. The user agrees never to access, possess, transmit, retransmit or respond to any information containing sexually oriented material.
16. The user agrees never 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.
17. The user agrees never to use the school and school affiliated network for commercial sales, multilevel marketing, gambling, sweepstakes, chain letters, or similar unauthorized purposes.
18. On-line games may only be accessed for educational purposes with the consent of the user's school personnel.
19. The user agrees to never 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.
20. The user agrees never to plagiarize. Plagiarism is defined as taking the idea or writing of others and presenting them as one's own.
21. The 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 bring this question immediately to the attention of a faculty member.
22. The use of blogs, wikis, podcasts, cloud storage (as it relates to sharing) or other social interactive web tools 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. This includes but is not limited to profanity, racist, sexist, or discriminatory remarks.

23. Students should only create a class blog or wiki for educational purposes and with permission of school personnel. Student profiles are not permitted to be used to create personal blogs or wikis. Never link to web sites from your blog, blog comment, or wiki without reading the entire article to make sure it is appropriate for a school setting.
24. The use of social networking sites by students, staff and faculty (e.g. Facebook, Instagram, etc.) for personal reasons are not allowed during school hours. *Please reference the Diocesan Social Media Policy*.

Specific Technology Use:

3D Printers

The Diocese provides students 3D printers, scanners and related equipment ("3-D printers") to use when there is a Diocese 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 student or employee to operate a 3D printer. If approved, the person approving such use must then supervise the students' use. The Diocese reserves the right to deny any request.

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); (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.

Students 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 enforce the regulations and/or rules to carry out the use of 3D printers.

Wearable Technology

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

The Internet of Things 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 or employees 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 (CIS Systems). They have no expectation of privacy in their personal files or any of their use of the Diocese's CIS Systems. The Diocese reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any or all CIS Systems use and

to monitor and allocate cloud and/or fileserver space. The Diocese does not attempt to collect the information on the wearers' devices.

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.

Students involved in 1:1 initiatives:

- Agree to the practices outlined in the Equipment Receipt and Use Agreement that was signed when he/she received his/her device.
- Non-functioning devices are not an excuse for lack of participation in class or failure to complete assigned work.
- Student should refer to the Help Desk guide on their website for guidance on how to receive technical help and support on their school provided electronic devices. Help Desk support is limited to school owned devices; no assistance will be given on personally owned devices.

Privileges and Enforcement

The use of electronic networks and technology is a privilege, not a right. Access is given to users who agree to the terms of this Acceptable Use Policy Agreement. Inappropriate use or a violation of this agreement may 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. 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. All e-mail communications remain Diocese property. The Diocese of Greensburg reserves the right for its authorized representatives as specified, with written approval from the Superintendent, to access, use and disclose the contents of e-mail files for legitimate 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 employee of the Diocese of Greensburg, or school or parish within the Diocese of Greensburg 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. School personnel will have the right to review any and all material saved, transmitted, accessed, or momentarily in use by the student in accord with the policy set by the school's administration. Users should not expect that files will be private (see Introduction, paragraph 1).

Liability

School Name 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 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

School Name makes no warranties of any kind, whether expressed or implied, for the service we are providing.

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

SCHOOL NAME TECHNOLOGY RESOURCE AND COMMUNICATION SYSTEM

PARENT / GUARDIAN PERMISSION TO ACTIVATE USER PRIVILEGES

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. As the parent of a student of the Diocese, I have received, read, and understand the Student Acceptable Use Policy Agreement. In addition, I reviewed it with my child and answered questions he or she asked. If either my child or I have further questions I will ask the school principal. If I need a copy of the Policy I understand that I can access it on the Diocese's website. I agree to have my child comply with the requirements of the Policy, other Diocese policies, regulations, rules, and procedures. Additionally, I understand that if (s)he violates the Policy, other Diocese policies, regulations, rules and procedures (s)he is subject to the school's/Diocese's discipline, Internet Service Provider's, website's, and app's rules, as well as local, state and federal laws and procedures. 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.

PARENT / GUARDIAN PERMISSION FOR WORLD WIDE WEB 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

I understand that my child's photograph and samples of my child's school work may be published in The Catholic Accent, the official newspaper of the Diocese of Greensburg, and on the school and/or Diocesan websites. 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 web site. I understand that I can request that my child's individual picture or school work not be published on the school web site. This is not inclusive of any group, class, or school production photos utilized on the web site 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 or on the Diocesan or school web site, I will submit written notification, including the date, child's name, and grade to the school principal.

STUDENT PERMISSION TO ACTIVATE USER PRIVILEGES

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 Agreement, 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 WORLD WIDE WEB 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, the official newspaper of the Diocese of Greensburg, and on the school and/or Diocesan websites.

PERMISSION TO ACTIVATE USER PRIVILEGES

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 School Name. 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 World Wide Web 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 web site.

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