

## STUDENT INTERNET USE POLICY

---

**Computer Policy Statement** - The following is a policy statement regarding the use of microcomputer software:

*The Diocese of St. Petersburg and Guardian Angels Catholic School purchase or license the use of copies of computer software from a variety of outside companies. The Diocese of St. Petersburg and Guardian Angels Catholic School do not own the copyright of this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer.*

*Employees, parents, volunteers, and students of schools and centers shall use software on local area networks and multiple machines only in accordance with the license agreement.*

*Employees, volunteers, and students learning of any misuse of software or related documentation within the school or center shall notify the school/center administrator or the Superintendent of the Diocese of St. Petersburg.*

*According to the US Copyright Law, illegal reproduction of software can be a serious offense punishable by fine and criminal penalties. The Diocese of St. Petersburg will not tolerate the use of illegal, pirated software. Any employee, parent, volunteer or student who makes, acquires or uses unauthorized software shall be disciplined as appropriate under the circumstances.*

### **Diocese of St. Petersburg Student Internet Use Policy**

This document sets forth the rights and responsibilities for students under the Diocese of St. Petersburg Student Internet Use Policy. This Student Internet Use Policy is, by reference, a part of the Student Internet Account Agreement which must be executed by each Student and each Student's Parent or Guardian.

#### **A. EDUCATIONAL PURPOSE:**

1. The school internet system has been established for a limited educational purpose. Educational purposes include classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research.
2. The school internet system has not been established as a public access service or a public forum. The Diocese and school has the right to place restrictions on the material you access or post through the school internet system. You are expected to follow the rules set forth in this policy, the student disciplinary code, and the law in your use of the school internet system. The student disciplinary code will govern any violations of this policy.
3. You may not use the school internet system for commercial purposes. This means you may not offer, provide, or purchase products or services through the school internet system.

#### **B. ACCESS TO ONLINE MATERIALS:**

1. The material you access through the school internet system should be for class assignments or for personal research on subjects you study in a class or would otherwise research in the school media center. Use for entertainment purposes is not allowed.
2. You are not allowed to use the school internet system to access inappropriate information, which includes, but is not limited to, the following: obscene material, child pornography, material which depicts or describes in an offensive way violence, nudity, sex, death, or bodily functions, material designated as for adults only, material which promotes or advocates illegal activities, material which promotes the use of alcohol or tobacco, school cheating, or weapons, or material advocating participation in hate groups or other potentially dangerous groups.
3. If you mistakenly access inappropriate information through the school internet system, you are required to immediately report this access in the manner specified by your school. This will protect you against a claim you have intentionally violated this policy.
4. The school has installed filtering software to attempt to prevent access to inappropriate material.
  - a. If you feel filtering software is blocking your access to an appropriate site, report this to your teacher.
  - b. You are not allowed to seek to bypass the filtering software by using a proxy site or some other technology.

### C. PRIVACY AND COMMUNICATION SAFETY REQUIREMENTS:

1. "Personal contact information" includes your full name, together with other information which would allow an individual to locate you, including your family name, your home address or location, your work address or location, or your phone number.
2. If you are an elementary or middle school student, you are not allowed to use the school internet system to disclose your full name or any other personal contact information online for any reason.
3. If you are a high school student, you may disclose, through the school internet system, personal contact information to educational institutions, companies or other entities for continuing education, professional or career development purposes with specific staff approval.
4. You are not allowed to disclose names, personal contact information, or any other private or personal contact information about other students. You are not allowed to forward a message sent to you privately without documented permission from the person who sent you the message.
5. You are required to promptly disclose to your teacher or other school staff member any message you receive through the school internet system which is inappropriate or makes you feel uncomfortable. You should not delete such messages until instructed to do so by a teacher or other staff member.

### D. UNLAWFUL, UNAUTHORIZED, AND INAPPROPRIATE USES AND ACTIVITIES:

#### 1. Unlawful activities:

- a. You are not allowed to attempt to gain unauthorized access to the school internet system or to any other computer system through the school internet system or go beyond your authorized access. This prohibition includes attempting to log-in through another person's account or to access another person's files.
- b. You are not allowed to disrupt or attempt to disrupt the school internet system or any other computer system or destroy data by spreading computer viruses, or by any other means, using the school internet system.
- c. You are not allowed to use the school internet system to engage in any unlawful act, including but not limited to arranging the sale or purchase of drugs or alcohol, engaging in criminal gang activity, or threatening the safety of any person.

#### 2. Inappropriate language:

- a. Restrictions against inappropriate language apply to all speech communicated through the school internet system, including public messages, private messages, and material posted on Webpages.
- b. You are not allowed to use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language on the school internet system.
- c. You are not allowed to post information which could cause damage or a danger of disruption to your school or any other organization or person on the school internet system.
- d. You are not allowed to engage in personal attacks, including prejudicial or discriminatory attacks on the school internet system.
- e. You are not allowed to harass or bully another person on the school internet system.
- f. You are not allowed to post false or defamatory information about a person or organization on the school internet system.
- g. You are required to promptly disclose to your teacher or another school employee any message you receive on the school internet system in violation of the restrictions on inappropriate language.

#### 3. Plagiarism and copyright infringement:

- a. You are not allowed to plagiarize works you find on the internet. Plagiarism is taking the ideas or writings of others, and presenting them as if they were yours, without proper attribution.
- b. You are required to respect the rights of copyright owners in your use of materials found on, disseminated through, or posted to the internet. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright.

#### 4. Specific Activities prohibited:

- a. Inappropriate activities subject to discipline under this policy include but are not limited to:
- b. The transmission of material, information or software in violation of school policy, or
- c. local, state and federal law,
- d. Changing of Windows/Mac platform settings (desktop, screensavers, etc.),
- e. Downloading software or plug-ins into the school internet system,
- f. The use of web-based email accounts,
- g. Online chatting or any instant messaging,
- h. Making purchases via the internet,
- i. The installation of any software on the system by a student. Software can only be installed by the school, using software purchased by the school and appropriately licensed by law for use on school computers, violating copyright or other laws, accessing personal files belonging to others, accessing areas of the network which are not designated for your use.

#### 5. Limited Privacy:

- a. You are notified by reading and signing this document that you have only a limited expectation of privacy in your files on the school internet system and in the records of your online activity. All student use of the school internet system may be supervised and is subject to being closely monitored at all times. You are notified that the school's monitoring of internet usage can reveal all activities you engage in using the school internet system.
- b. Routine maintenance and random monitoring of the school internet system may disclose information indicating you have violated this policy, the student disciplinary code, or the law. A detailed search of your individual school internet system account, and its historical activity, may be conducted if there is reasonable suspicion you have violated this policy, the student disciplinary code, or the law.

### E. SYSTEM SECURITY AND RESOURCE LIMITS:

#### 1. System security:

- a. You are responsible for your school internet system individual account and should take all reasonable precautions to prevent others from being able to use your account. You should not provide your password to another person.
- b. You are required to immediately notify a teacher or the system administrator if you have identified a possible security problem involving the school internet system. However, you are not required to look for security problems; this may be construed as an unlawful attempt to gain access.
- c. You are required to avoid the inadvertent spread of computer viruses by following the school virus protection procedures.

#### 2. Resource limits:

- a. You are required to use the school internet system only for educational, professional or career development activities and limited, high-quality personal research.
- b. You are not allowed to download large files from or to any computer on the school internet system unless absolutely necessary, and then only with approval of a teacher or another school employee. If necessary, and allowed, you may download large files when the system is not being heavily used; you are required to immediately remove the file from the school internet system computer as soon as possible after appropriate copying or use.
- c. You are not allowed to use Diocesan, school, or personal distribution lists or discussion groups for sending irrelevant messages.

## F. DISCIPLINE

Violations of this Student Internet Use Policy can result in termination of the student's account, denial of access to the school internet system, suspension, expulsion, or referral of matters to the appropriate law enforcement agency, depending on the severity of the actions. Such determination is within the sole discretion of the school and the diocese.

## G. LIMITATION OF LIABILITY:

Neither the diocese nor school guarantees the functions or services provided through the school internet system and its internet service provider, will be without error. The diocese and/or school will not be responsible for any damage you may suffer, including but not limited to loss of data, interruptions of service, or exposure to inappropriate material or people. The diocese and/or school will not be responsible for the accuracy or quality of the information obtained through the school internet system. The diocese and/or school will not be responsible for financial obligations arising through the unauthorized use of the school internet system. Your parents can be held financially responsible for any harm resulting from your use or misuse of the school internet system. You may use the school internet system only if your parents have signed a disclaimer of claims for damages against the school and diocese.

## **Student Internet Account Agreement**

### **I. Student Section**

By signing the Internet Use Policy Agreement Form, I state that, I have read the Diocesan Student Internet Use Policy and the Wireless Network Internet Access Policy which is made a part of this Agreement, by reference. I agree to follow the rules contained in this policy. I understand if I violate the rules, my account can be terminated and I may face other disciplinary measures.

### **II. Parent or Guardian Section**

By signing the Internet Use Policy Agreement Form, I agree that I have read the Diocesan Student Internet Use Policy, which is made a part of this Agreement, by reference. I hereby release the Diocese and school, its personnel, and any institutions with which it is affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the school internet system, including but not limited to claims arising from the unauthorized use of the system to purchase products or services or exposure to potentially harmful or inappropriate material or people. I understand I can be held liable for damages caused by my child's use or misuse of the school internet system.

I will instruct my child regarding restrictions against accessing material in addition to the restrictions set forth in the Diocesan/school policy. I will emphasize to my child the importance of following the rules for personal safety.

By signing the Parent Form, I agree that I hereby give permission for my child to use the school internet system. I understand this permission includes permission for my child to access information on-line through the World Wide Web, receive e-mail communications through a class account or individual e-mail account, if applicable, and engage in other educationally relevant electronic communication activities.

## **Wireless Network Internet Access Policy**

Students are expected to abide by both aforementioned policies.

### **1. Purpose**

Use of wireless mobile learning devices (WMLD) are becoming increasingly prevalent in education.

These devices can greatly supplement and enhance the academic learning environment. Your teacher has asked for student use of WMLD as an instructional aide to add to the student learning process. For this reason the internet access use policy addendum needs to be added.

### **2. Policy**

While in some instances the possession and use of WMLDs by students at school may be appropriate,

the possession and use of such devices or objects by students at school can have the effect of distracting, disrupting, and intimidating others in academic setting and leading to opportunities for academic dishonesty and other disruptions of the educational process. The purpose of this policy is to vest with school administrators and staff the authority to enforce reasonable rules relating to student use of such objects or devices at Guardian Angels Catholic School.

### ***Background***

Guardian Angels Catholic School offers wireless internet access for school owned and personally owned devices (POD). In addition, the Guardian Angels Catholic School wireless network utilizes a WPA2 wireless security protocol.

## **3. Procedure**

### **3.1. Definitions:**

**3.1.1. Acceptable Use:** Students are not permitted to use any type of WMLD during class time, passing periods or breaks without the permission of the teacher or school administration. All WMLDs must remain turned off and out of sight while on campus. Some teachers may allow students to use these devices in class, but such use should not disrupt the learning environment and must conform to the policies set forth.

**3.1.2. Prohibited Use:** Any use that violates local, state and/or federal laws.

### **3.2. Prohibited Uses:**

Students are not to use material, images or text message to invade personal privacy or harass another person, or disrupt the instructional day, or engage in dishonest acts. The following are inappropriate uses of electronic WMLDs:

**3.2.1. Harassment, threats, intimidation, cyber bullying/cyber threats of other students, teachers, staff or school administration via cellular phone calls, SMS text messaging or by the use of MMS picture messaging.**

**3.2.2 Passing or transmitting otherwise secure information, i.e. electronic forgery.**

**3.2.3 Invasion of personal rights in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, restrooms, and any other areas where students or others may change or be in any stage or degree of disrobing or changing clothes.**

**3.2.4 Cheating on tests/exams by either transmitting or receiving test/exam information or images before, during, or after the administration of the test/exam.**

**3.2.5 Violation of any other school policy or other forms of illegal behavior during the instructional and non- instructional day.**

**3.2.6 Image capture or intended image capture anywhere on the campus of Guardian Angels Catholic School either indoors or outdoors, without administrative approval. "Image capture", "photography" and videoing" refer to any kind of image capture, still or moving, obtained by any photographic device including still image cameras, video cameras, CCTV cameras, webcams and photographic/video enabled cell phones, and any other type of image capture device not specified here, whether digital or not, using technology existent at this time or in the future. In addition, the uploading of said images to public venues, such as social networking sites.**

### **3.3. Privileges and Discipline:**

**3.3.1 Students may have WMLDs in their possession or in their lockers at other times as long as the device is powered down and the device is out of sight in a pocket, bag or backpack.**

**3.3.2 If a student receives permission by a teacher or school administration to use a WMLD, it shall not disrupt the educational program.**

**3.3.3** If disruption occurs, the school staff shall direct the student to turn off the WMLD and confiscate it. In the event a school staff member finds it necessary to confiscate a device, it will be returned in accordance with school policy as stated in the Guardian Angels Catholic School Parent/Student Handbook.

#### **4. Non-Employee Use**

Each time someone accesses the Guardian Angels Catholic School wireless network (GACSWN), they agree to the terms listed below.

##### **Terms**

Guardian Angels Catholic School will not be held liable for any damage that may occur as a result of connecting to the GACSWN or any electrical power source.

Guardian Angels Catholic School will not be held responsible for any physical damage, loss or theft of the personally-owned device.

The GACSWN will provide filtered internet access and related web-based services only.

Guardian Angels Catholic School reserves the right to inspect, at any time, any personally-owned device while connected to the GACSWN. Any other inspection of any personally-owned device is subject to the requirements set forth in the Guardian Angels Catholic School Parent/Student Handbook.

Personally-owned WMLDs will only be connected to the network at designated locations.

Guardian Angels Catholic School will not be obligated to supply electrical power access where such access does not already exist.

Persons connecting computers to the GACSWN agree to maintain current anti-virus software enabled on said devices.

Illegal, destructive, harmful or any other inappropriate activities, including, but not limited to computer hacking, cyber-bullying, accessing offensive/obscene materials, engaging in illegal activity are strictly prohibited as set forth in Guardian Angels Catholic School Parent/Student Handbook and local, state and federal laws.

The parents and/or guardians of any student bringing personal technology to school agree to be responsible for and to reimburse Guardian Angels Catholic School for any damage that their student may cause arising out of and relating to the use of the GACSWN with his/her personally owned device.

#### **6. Monitoring**

Through the use of sophisticated hardware, all users accessing the internet through the Guardian Angels Catholic School wireless network will be monitored and all website activity tracked.

Any WMLD accessing inappropriate material on the internet will be added to a device blacklist, preventing future connection to the Guardian Angels Catholic School wireless network.

#### **7. Enforcement**

The Guardian Angels Catholic School administration reserves the right to pursue legal recourse for activities conducted upon the devices and networks utilized in the education setting on campus in which it deems inappropriate or illegal by local, state and federal laws. Any abuse of the law will be immediately reported to law enforcement