

**DIOCESE OF ALLENTOWN**  
**St. Theresa of the Child Jesus School in Hellertown Pennsylvania – hereafter referred to as St. Theresa School**  
**ACCEPTABLE USE POLICY**  
**For**  
**USE OF THE COMPUTERS, NETWORK, INTERNET,**  
**ELECTRONIC INFORMATION AND COMMUNICATIONS**

*Please read the following carefully before signing this document. This is a legally binding document.*

**SECTION ONE: GENERAL, COMPUTING POLICY**

**Overview**

Computers, hand-held devices, network, Internet, electronic communications and information systems (collectively “CIS systems”) provide vast, diverse and unique resources. Access to the School’s electronic communication systems and network is granted to responsible users for educational purposes, and terms of use are outlined in this document. This access includes Internet access, whether wired or wireless, or by any other means.

**1) Acceptable Use**

In order to ensure smooth system operations, the system administrator has the authority to monitor all accounts. A user must abide by the terms of all software licensing agreements and copyright laws. A user can be monitored at any time. When a user receives a user ID to be used to access a computer or network and computer systems on that network, he or she is solely responsible for all actions taken while using the user ID. Therefore the following are prohibited:

- a) Sharing your user ID with any other person. (If you do share your user ID with another person, you will be solely responsible for the actions of that other person)
- b) Deletion, examination, copying, or modification of software programs, files, and/or data belonging to the school or other users without prior written consent
- c) Attempts to make unauthorized use or modifications to St. Theresa School WEBSITE, Teacher WEB content Pages, or student related content pages or Websites that are created while participating in curriculum activities at the school. Such attempts outside of school are covered by State Criminal Codes and are considered criminal acts and will be referred to the appropriate legal authorities.
- d) Attempts to evade or change resource quotas
- e) Use of facilities and/or services for commercial purposes, unless approved by the school Principal as part of regularly approved school fund raising activities.
- f) Any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation, regardless of system location or time duration
- g) Copying programs purchased by you onto St. Theresa computers and/or the network systems, without the express, written consent of the principal of St. Theresa School.
- h) Copying programs licensed St. Theresa School for personal use.
- i) Abusing and disrupting any of the schools technology resources, equipment and/or systems.

## 2) Security

As a user of a computer or network, you may be allowed to access other networks and/or computer systems attached to those networks. Therefore the following are prohibited:

- a) Use of systems and/or networks in attempts to gain unauthorized access to remote systems-- this includes all proxy servers, cloud based services not approved by the school, and illegal download tools and sites.
- b) Decryption of system or user passwords – Use of tools that decrypt passwords and other security protocols
- c) Copying, deleting, or moving system files – without the expressed permission of the classroom teacher, technology coordinator, or school principal.
- d) Deleting, examining, copying, or modifying files and/or data belonging to other users – This includes students data stored on student Flash Memory Devices.
- e) Copying of copyrighted materials, such as third- party software, without the express written permission of the owner or the proper license – This also includes copyright violations of any copyright protected content, not just software. Fair Use Provisions of the Copyright laws, Creative Commons Licensing, General Public Licensing, and Public Domain software and content are not considered copyright violations and students should be directed to using these appropriate resources.
- f) The willful introduction of computer "viruses", "spyware" or other "malware" disruptive or destructive programs into the computer and/or network or into external computers and/or networks
- g) Vandalism is prohibited. This includes, but is not limited to, any attempt to harm or destroy the data of another user, the network/Internet, or any networks or sites connected to the network/Internet. Attempts to breach security codes and/or passwords will also be considered a form of vandalism.
- h) Willful destruction of computer hardware or software, or attempts to exceed or modify the parameters of the system are prohibited. Nothing in this policy shall prohibit the school/institution operator from intercepting and stopping E- mail messages or other types of electronic messaging which have the capacity to overload the computer resource. If students are found to be participating in DOS (Denial of Service) attacks on a school system or are participating in such acts outside of school using school resources, they are in violation of criminal statues and will be referred to the appropriate legal authorities.

## SECTION TWO: INTERNET ACCESS

Internet access is now available to employees and students of St. Theresa School. This access is being offered as part of a collaborative project involving St. Theresa School, the Diocese of Allentown WAN, and Penteledata Services the school's current Internet Service Provider (ISP) We are pleased to bring this access to **St. Theresa School** and believe the Internet offers vast, diverse and unique resources to administrators, teachers, employees, and students. Our goal in providing this service is to promote educational excellence at St. Theresa School by facilitating resource sharing, innovation and communication.

The Internet is an electronic highway connecting millions of computers all over the world and millions of individual subscribers. Administrators, teachers, employees, and students have access to:

- \* electronic mail communication with people all over the world;
- \* access to many University Library Catalogs, the Library of Congress, and ERIC or other academic databases, public domain and open source software of all types;
- \* information and news from NASA, as well as the opportunity to correspond with the scientists at NASA and other research institutions.
- \* online learning communities where academic collaboration and discussion are encouraged;
- \* institutions of higher academic learning where students may earn college credits which will satisfy academic requirements towards baccalaureate degrees.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the school setting. St. Theresa School has taken precautions, which are limited to known sites, to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. We, **St. Theresa School** firmly believe that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of this Project.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical and legal utilization of the network resources. If a **St. Theresa School** user violates any of these provisions, his or her account will be terminated and future access could possibly be denied. Disciplinary or legal action including, but not limited to, criminal prosecution under appropriate state and federal laws may also be taken. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

## INTERNET ACCESS - TERMS and CONDITIONS

### 1) Acceptable Use

The purpose of accessing the Internet is to support research and education in and among academic institutions in the United States and globally by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and research, and consistent with the educational objectives of St. Theresa School. Each user is personally responsible for this provision at all times when using the network.

- a) Use of other organization's network or computing resources must comply with the rules appropriate for that network.
- b) Transmission of any material in violation of local, state, and/or federal statutes or regulations is strictly prohibited. This includes, but is not limited to: copyrighted material, material protected by trade secret, threatening or obscene material, and criminal activity.
- c) Use by student users for commercial activities or product advertisement (including campaigns for student government/council) is prohibited unless prior written approval is obtained from the school principal. This activities must demonstrate that they are designed to enhance the school community and its overall experience and are not designed for personal gain or aggrandizement.
- d) Do not use the network in any way that would disrupt network use by others.
- e) **NEVER** reveal personal information, such as your address, phone number, password, or social security number. This also applies to others' personal information or that of organizations.
- f) Use of the network or computer resources to publicly oppose, degrade, or intentionally misrepresent any teachings, beliefs, or practices of the Catholic Church are strictly prohibited.
- g) Use of the network or computer resources to publicly embarrass, degrade, or intentionally bring harm or harassment to a fellow student or member of the school community is strictly prohibited and is considered "Cyberbullying". Threats on the life of any school community member, threats of destroying any property associated with **St. Theresa School or St. Theresa Parish**, or threats regarding any publicly elected official and/or any group or organization, or on our nation are considered potential cyber crimes and will be referred to the appropriate legal authorities.

### 2) Privileges

***The use of the Internet is a privilege, not a right***, and inappropriate use will result in a cancellation of those privileges. (Each student who receives an account will be a part of a discussion with a St. Theresa School faculty member pertaining to proper use of the network.) The system administrator will deem what is inappropriate use and his or her decision is final. Also, the system administrator may close an account at any time. An administrator, faculty member, or staff of St. Theresa School has the right to request, for cause, that the system administrator deny, revoke, or suspend specific user accounts.

### 3) Network Etiquette

You are expected to abide by the generally accepted rules of network etiquette (netiquette). These include, but are not limited, to the following:

- a) Be polite. Do not send, or encourage others to send, abusive messages
- b) Use appropriate language. Remember that you are a representative of your school and district on a non-private network. You may be alone on a computer, but what you say can be viewed around the world. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
- c) All communications and information accessible via the network should be assumed to be private property.

#### 4) Electronic Mail (E- Mail)

Whenever you send electronic mail, your name and userID are included in each message You are responsible for all electronic mail originating from your userID. Therefore:

- a) Unauthorized attempts to access another person's E- mail or similar electronic communications or to use another's name, E- mail or computer address or workstation to send E- mail or similar electronic communications is prohibited and may subject the individual to disciplinary action.
- b) All users must understand that the school/institution cannot guarantee the privacy or confidentiality of electronic documents and any messages that are confidential as a matter of law should not be communicated over the E- mail
- c) The school/institution reserves the right to access E- mail to retrieve school/institution information and records. to engage in routine computer maintenance and housekeeping, to carry out internal investigations, or to disclose messages, data or files to law enforcement authorities.
- d) Any information contained on a school/institution computer's hard drive or computer disks which were purchased by the school/institution are considered the property of the school/institution.
- e) Forgery (or attempted forgery) of electronic mail is prohibited.
- f) Attempts to send harassing, obscene and/or other threatening e- mail otherwise known as "Cyberbullying" to another user is prohibited.
- g) Attempts at sending unsolicited junk mail, "for profit" messages or chain letters is prohibited.

#### 5) Security

Security on any computer system is a high priority, especially when the system involves many users. Never use another person's account to log on to the system. If you feel you can identify a security problem, you must notify the system administrator, or send an e- mail message to St. Theresa School. Do not demonstrate the problem to other users. Do not reveal your account password to anyone. Users are responsible for any misuse of their account that is due to their own negligence. Users are responsible for reporting unauthorized use of their account to the system administrator.

#### 6) Updating Your User Information

**If any information on your account changes, i.e., telephone number, location, home address, it is your responsibility to notify the system administrator. The school's Information Management System (Option C – Option Catholic) is managed by an outside resource and is a Cloud Based Service to this school. While the school maintains procedures to protect student data, the data is housed externally and is not housed within the school. All data is password secured and is backed up by the school IMS provider. The need to have current information available in the case of an emergency is vital to the operation of the school. Please see that all required information on students and families is provided by you within 72 hours of those changes so that the school records may remain current. All registered school families receive login and password access to the IMS system data on their child(ren). These Logins and Passwords should not be shared with anyone outside the family members you have identified as being allowed to see this data in our school records.**

#### 7) Services

Diocese of Allentown and **St. Theresa School** make no warranties of any kind, whether expressed or implied, for the service it is providing. St. Theresa School and will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non- deliveries, mis▼deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the system is at your own risk. St. Theresa School specifically denies any responsibility for the accuracy or quality of information obtained through its services.

## 8) BYOD (Bring Your Own Device) Policies and Procedures:

**St. Theresa School** has operated a limited BYOD policy for specific class related projects for the past four years. BYOD devices include, but are not limited to: laptop, netbook, ultrabook, chromebook, tablet, iOS and Android platform mobile devices, cell phones and smart phones, Google Glass, MP3 and MP4 Audio and Video Players, and DS and other mobile game systems with Wifi capability. As of the 2012-2013 school year the use of BYOD devices for specific academic projects were expanded to include students in grades 4 through 8. The school also provides Wifi Guest access to other educators and Parish members using the school facilities. The purpose for all BYOD activities at the school is for the enhancement of some specific educational project. BYOD devices are not permitted to be used on school property for any activity unrelated to specifically assigned educational tasks or projects. Teachers and Technology Staff along with the school principal at **St. Theresa School** must approve all BYOD project activities. The school provides mobile technology for use at the school with all grades so that students are not compelled to use BYOD devices for any school related project or activity.

### **BYOD Use Procedures:**

1. Students must receive a specific assignment and/or project activity before being allowed to use their BYOD device.
2. BYOD devices may only be used on school property where the activity or project is taking place, unless the project or activity involves a supervised field trip where the devices are being used to document the field experience.
3. BYOD devices are to be kept in the student's locker or in their personal possession at all times and are only to be taken out during the specific project or activity.
4. Once the activity or project is completed for that assignment the BYOD device must be put back in the locker or put away in a book bag until it is required for use again.
5. In the event of a school emergency, and only where authorized by the principal of the school students may use BYOD devices to notify parents of their safety and status.
6. Students are responsible for the care and management of all BYOD devices at all times. At no time is the school staff responsible for these devices. In keeping with this procedure, no **St. Theresa School** staff member is to handle a student's BYOD device.
7. Students are responsible for the care and management of all BYOD devices when transporting to and from the school. Students are to follow transportation provider policies in regard to the use of their BYOD devices while using the transportation service.
8. All student BYOD device users are required to have Anti-virus Protection and other malware protection on their BYOD device before it is used in the school. The Technology staff will inspect the device while the student is handling it to determine what product is being used and whether the product is up to date. Students must update all product protection software prior to using it in the school. No specific product is required – students and their families should decide on the protection product(s) to be used.
9. The school is not liable for the student using their BYOD device to access any content that would be in violation of the school's normal acceptable use policy provisions when on school property but not accessing the school's Wifi network. Content already on the device before it is brought to school is the property of the BYOD device user and that user is responsible for how that content is used when on school property. When a BYOD device accesses the school's Wifi network the school's content filtering will be applied to that device. A student using 3G or 4G data services to access Internet Data, Content or Programs is responsible for their own use of that service. If they violate the other provisions of the school's AUP when using those phone services they will be prohibited from using their BYOD devices in the school again.
10. At no time is a student or teacher permitted to Text to each other except where the texting is part of a student classroom response activity in which the BYOD device is being used. Students may not send text messages to each other unless it is specially part of a classroom assignment activity.
11. Students and teachers may not use BYOD devices to send personal email messages, to send personal photographs or videos to each other, or to do any "face-time" activities using their BYOD devices.
12. Students violating any of the provisions or procedures above, will have the following consequences applied for inappropriate BYOD use:
  - a) First offense – Verbal warning and written notice to the parents of the verbal warning and the infraction in the AUP.
  - b) Second offense – Verbal warning, written notice to the parents, and the device will be retained by the principal until the close of the school day.
  - c) Third offense – Verbal warning, written notice to the parents, and the device will be held by the principal until the end of the day – No further BYOD use will be permitted for the remainder of the school year for that student.

***Fines will no longer be imposed as of the revision of this AUP, but BYOD use will be strictly prohibited for any user who has committed a third offense.***

## **General Consequences for Violations of this AUP**

1. For any offense involving the destruction or the damage of any technology equipment and/or software the student committing the damage will be restricted for all school technology use for the remainder of the school year. BYOD use may be permitted by the principal.
2. For any offense involving the misuse of any technology resources or equipment the following actions will be taken:
  - a) First offense – Verbal warning and written notice sent to the parents
  - b) Second offense – Verbal warning and written notice sent to the parents, and a one week suspension from the use of all school technology resources.
  - c) Third offense – Verbal warning, written notice to the parents, and the suspension from the use of all school technology resources for one school quarter
  - d) Fourth offense – Verbal warning, written notice to the parents, suspension of all technology resource use for the remainder of the school year.

## **Special AUP requirements for 3D printing technology in the school:**

**St. Theresa School** has acquired 3D printing technology. This technology is provided to enhance the student's creativity, to provide opportunities to learn more about 3D modeling in ART and for STEAM (Science Technology Engineering, Math and the Arts) projects. It is also available for teachers to be able to create 3D objects that will enhance student understanding of key concepts in all curriculum areas. The technology may also be used for students to create objects that they may use for School Science Fair activities, and school fund raising projects. This technology will not be used for the student to create personal items for use outside of school. The students will be required to follow all copyright provisions when considering using 3D designs that are available on the Internet for use with 3D printers.

Due to the very expensive nature of this technology students may be charged a fee for creating project objects that use a significant quantity of printer materials, or the student may be asked to purchase their own materials for use with the printer. Fees and/or purchase of their own materials will be determined by the size, complexity, and density of the project materials required to complete the project successfully.

Students may only use the 3D printing technology when being supervised by trained staff within the school. At no time may the student use this technology on their own.

Students damaging this equipment will be responsible for the full replacement cost of any parts and/or the whole of this 3D printer and materials.

## **School Email and WEB 2.0 Collaboration Tool Usage**

The school maintains Email address access for all teachers and staff. These email addresses are only to be used for professional school communications and are not to be used for personal communications. At no time is a staff member to use personal email to communicate with a student.

The school utilizes the ePals – secure and monitored email and related services for all students in grades 3 through 8. Parents must sign a special approval form for students not previously registered with ePals, if the student is under 13 years of age. Forms may be obtained from the school Technology Coordinator. Students are not permitted to use personal email account information in school except when assigned to use and educational WEB 2.0 tools that require email registration. Students must have prior written permission from their parents to be allowed to use personal email information for registration for educational WEB 2.0 collaboration tools.

The school uses the following WEB 2.0 collaboration tools which are secure and monitored by the teaching staff:

Edmodo, Skype for Classrooms, Teacher Tube and School Tube, Wikispaces for Classrooms, Scholastic Classrooms, Discovery Education Network (which includes PBS Teachers tools), Diigo, and Google Apps. Teachers will notify parents when these tools or other collaborative WEB 2.0 educational tools are being used for a specific class project.

There is a School Facebook page and families are encouraged to sign up for that page; however students at this school are not permitted to use Facebook accounts during school hours. Teachers are permitted to demonstrate Twitter as an educational tool and demonstrate its effectiveness for teaching precise writing and for gathering professional and educational information resources, however students at this school are not permitted to use Twitter at school even if they have a Twitter account. Twitter is considered an acceptable educational tool in many schools across the nation, but is primarily used in High School settings. St. Theresa School does not endorse the use of Twitter as a regular classroom educational tool for students under 13 years of age or younger. Teachers may use WEB 2.0 secure and monitored “Twitter like” tools in place of Twitter for precise writing activities.

***Our school participates in local, regional, national and global collaborations using the tools mentioned above with other schools and classrooms. Parents will be notified of these activities and of the guidelines for student participation in these collaborations.***

#### **Cloud Based Services and Storage:**

Teachers and students have the option of using Cloud Based (Online /Internet) storage for their data files. Some teachers establish Cloud based storage folders for student assignments. This is optional and no student needs to participate in the use of these services. The services selected are always free and there is no charge to the student or parent.

#### **Required Student Flash Memory Storage Devices**

***Students in grades 3 through 8 are required to have Flash Drive / Thumb Drive mobile storage for all data files created at school as these files are no longer stored on the school's network or on the school computer's hard drives. All computer systems in the school will be equipped with virus scanning software to scan Flash Drives before they are used on any of the school's computer systems. Students should scan their flash drives for viruses when using them on their BYOD devices.***

#### **Cloud Based Applications and Educational Software:**

Many of the educational activities done at this school utilize Internet based software and are not locally installed applications on the school's network servers. Much of this online educational software is provided by the Diocese of Allentown as part of the Diocesan Wide Area Network Project. Some of this software does require student login and passwords be assigned by the teacher. This software can be accessed both in school and at home. We strongly encourage parents to become familiar with these software tools and for parents to assist their children to use these tools to practice and strengthen skills used at home. The Diocese has made a significant financial investment in providing this software to the Diocesan schools and we want to encourage its use throughout the school year. Teachers will send information home regarding the student logins and passwords for this software. When using Diocesan Purchased Internet software at home all AUP policies apply to that software usage.

#### **Distance Education Activities**

St. Theresa School has initiated a program of Distance Education in cooperation with Bethlehem Catholic High School for the teaching of the Spanish Language. This Distance Education program will use standard Distance Education tools such as Blackboard, and Moodle along with Skype to allow for full participation in this program by the St. Theresa School students. The Diocese of Allentown owns the Blackboard and Moodle servers that will be used for this course. Those servers are housed and maintained at IU 20 in Tatamy. Students will be given specific logins and passwords to access these servers for their classes and for completing class assignments after the class is over for the day. These classes will run three to four days a week. Students will be required to follow all AUP policies of the Diocese and of St. Theresa School in regard to the use of these servers in order to participate in this program. We are excited about this opportunity for the students to participate in this activity, but require that the students understand that they are using Diocesan resources and not school resources and it is essential they understand that all school AUP guidelines and all Diocesan AUP guidelines apply to the use of those servers for this course. The Diocese of Allentown will be responsible for enforcing any AUP policies that apply specifically to the use of these servers for this class.

Adopted by St. Theresa School, 300 Leonard Street, PA on 8/26/2013

*Principal's Signature:*

*President of the School Advisory Board's Signature:*

*Pastor's Signature:*

*The Department of Education of the Diocese of Allentown would like to thank Bishop O'Reilly High School, Kingston, PA, the Luzerne Intermediate Unit #18, and the Diocese of Galveston-Houston for their assistance in developing this Acceptable Use Policy.*



## APPLICATION FOR INTERNET ACCOUNT

Complete this page and return it along with the signature sheet to:

System Administrator

St. Theresa School

300 Leonard Street

Hellertown, PA 18055

User's Full Name (please print)

Home Address

City/State/Zip

Home Telephone (        )

Work Telephone (        )

### CHECK ONE AND COMPLETE THE REQUESTED INFORMATION:

\_\_\_\_\_ I am a student in grade \_\_\_\_\_ at St. Theresa School

---

\_\_\_\_\_ I am a teacher at St. Theresa School

\_\_\_\_\_ I am an administrator at St. Theresa School

---

\_\_\_\_\_ I am an employee at St. Theresa School

---

When your account is established, you will be notified of your login name and user password.  
Thank you for your interest in and support of this exciting resource at St. Theresa School.

---

**St. Theresa School**  
**Agreement for the Use of**  
**Computers and Telecommunications**  
***Parental Consent Form***

St. Theresa School has chosen to permit students access to computer and telecommunication resources to further its educational goals and objectives. Reasonable care has been taken to assure the appropriateness and educational quality of the material available thorough the use of educational software and telecommunications. However, parents and guardians are warned that St. Theresa School and the Diocese of Allentown do not have total control of the information on the Internet. Parents and guardians are the primary authority responsible for imparting the standards of ethical and legal conduct their child or ward should follow. Therefore, St. Theresa School *supports* and respects each family's right to decide whether or not their child may have access to this resource. ▼

1. I am the parent/guardian of the below named student. I have read the Acceptable Use Policy for Computers and Telecommunications ("the policy") and I have either explained it to my child/ward ("student") or I have assured myself that the student understands it. I also understand my own and the student's responsibilities regarding computer hardware, software, and Internet access at .St. Theresa School.

2. Check one:

I hereby consent to the student having access to, and use of, the telecommunications resources at St. Theresa School, I also hereby indemnify and hold harmless The Diocese of Allentown and St. Theresa School from any claim or loss resulting from any infraction by the student of the policy or any applicable law.

I do not consent to the student having access to, or use of, the telecommunications resources at St. Theresa School.

---

Parent's/Guardian's signature

Date

---

Name of Parent/Guardian (Please Print)

---

Name of Student (Please Print)

---

Street Address

---

City/State/Zip

---

Home Phone

Cell Phone

**St. Theresa School  
Agreement for the Use of  
Computers and Telecommunications**

***Faculty/Staff/Volunteer Form***

I have read the Acceptable Use Policy for Computers and Telecommunications ("the policy"), I understand its significance, and I voluntarily agree to abide with all terms and conditions of it, imposed by the policy. I further understand that any violation of the policy or any applicable law or of this agreement would be unethical and might even constitute a criminal offense. Should I commit any such violation, I understand that my privileges will be revoked, and disciplinary action, and/or appropriate legal action may be taken. I also hereby indemnify and hold harmless The Diocese of Allentown St. Theresa School from any claim or loss resulting from any infraction by me of the policy or any applicable law.

---

User's Signature

Date

---

Name of User (Please Print)

---

Job title or position

---

Street Address

---

City/State/Zip

---

Home Phone

Office Phone

**St. Theresa School  
Agreement for the Use of  
Computers and Telecommunications**

***Student Form***

I have read the Acceptable Use Policy for Computers and Telecommunications, I understand its significance, and I agree to voluntarily abide with all terms and conditions of it. I further understand that violation of this agreement would be unethical and might even constitute a criminal offense. Should I chose to violate this agreement, my privileges will be revoked, and disciplinary action, and/or appropriate legal action may be taken.

---

Student Signature

Date

---

Name of Student (Please Print)

---

Name of Parent/Guardian (Please Print)

---

Street Address

---

City/State/Zip

---

Home Phone

Parent's/Guardian's Office Phone

**SPONSORING TEACHER** (Must be signed if the applicant is a student.) I have read the Terms and Conditions of this agreement, the Acceptable Use Policy for Computing and Internet Access, and agree to promote this agreement with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held responsible for the student's use of the network. As the sponsoring teacher, I do agree to instruct the student on the acceptable use of the network and proper network etiquette.

Teacher Name (please print) ▼ \_\_\_\_\_

Teacher Signature \_\_\_\_\_

Date ▼ \_\_\_\_\_