Union Parish School Board
Acceptable Use Policy and Internet Safety Agreement
Approved and Adopted August 14, 2012

Statement of Purpose

Union Parish School Board is pleased to offer our employees and students access to the World Wide Web and other electronic networks. The advantages afforded by the rich, digital resources available today through the World Wide Web outweigh any disadvantage. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved. **This policy applies to all persons who gain access with any device, whether personal or district provided, to the school network.**

Terms of Agreement

This policy applies to all persons using the Union Parish School Board network, accessing the Internet, or using a Union Parish School Board computer system. In order for a student/minor to be allowed access to a school computer system, computer network, and the Internet, parents must sign and return the attached consent form by September 1, 2012. For the purpose of this policy a minor is defined as an individual who has not attained the age of 17 years.

Acceptable Uses

The District is providing access to its school computer systems, computer networks, and the Internet for **educational purposes only**. The board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the school to help you decide. Accordingly, regulations for participation by anyone on the Internet shall include, but not be limited to, the following:

a) All users must abide by rules of Network etiquette – Netiquette, including the following:
- Be polite. Use appropriate language and graphics. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language. Personal attacks are an unacceptable use of the network. If a user is the victim of a harsh, critical, or abusive statement, the user should bring the incident to the attention of the immediate supervisor or technology coordinator. It is better not to respond to these types of attacks.
- Avoid language and/or graphic representations which may be offensive to other users. Don't use network or Internet access to make, distribute, or redistribute jokes, stories, or other material which is based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
- Do not assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.

b) Teachers may NOT allow individual students to use personal email, electronic chat rooms, instant messaging, social networking sites (I. E. Facebook and MySpace) and other forms of direct electronic communications. Webmail is NOT permitted on any computer located in the classroom or used by students except for school- provided student accounts that are educationally sound and safe that functions similar to that which is provided by services such as Gaggle. The teacher will use due diligence to monitor and insure the safety/security of minors when using Gaggle email, chat rooms, or other direct electronic communications.

c) No personal addresses, personal phone numbers, or last names of minors will be permitted to be given out on the Internet or for any type of student account. No identifiable photographs will be allowed to be published on the Internet without appropriate written consent. Concerning a student/minor, appropriate written consent means a signature by a parent or legal guardian of the student.

d) A student may not attempt to access any Internet resource without the prior consent of the teacher. The Internet is an extension of the classroom, and teachers are responsible for and must be aware of where his/her student goes on the Internet. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.

e) Students encountering information or messages they deem dangerous or inappropriate on the web or when using electronic mail or direct communications should notify their teacher other adult faculty member.

f) **Student Photos/Student Work**. Publishing student pictures and work on websites promotes learning and collaboration and provides an opportunity to share the achievements of students. Images and products of K-12 students/minors may be included on the website without identifying captions or names. Parents/guardians must indicate their written consent to publish their child's photo or school work on any school-related website BEFORE the item is

published to the web. Please note that under no circumstances will K-12 student photos or work be identified with first and last name on a Union Parish website, including the district, school, or teacher website.

Privacy. *Network and Internet access is provided as a* tool for your education. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District and no user shall have any expectation of privacy regarding such materials.

Copyright. All students and faculty must adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information.

Network Access. Access to the school network is a privilege, not a right. Every school in the district relies on the district network; therefore, preserving the integrity of that network must come first. The use of a personal wireless access points or routers is restricted, as their use causes network instability. The district technology department **must** be notified **before** connecting any device, such as but not limited to, smartphones, tablets or laptops, to the school network to prevent network problems.
No one may use any device to create a "hot spot", such as but not limited to, MYFI, that will allow an Internet connection that does not use the district's filter system. These devices allow access to web sites that are inappropriate to an educational environment.

Failure to Follow Acceptable Use Policy

The network is provided for students to conduct research, complete assignments, and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner. Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network and Internet terminated and is subject to disciplinary action by the school administrator. The District may also take other disciplinary actions. Listed below are examples of unacceptable uses of the network.

a) Uses that cause harm to others or damage to their property are prohibited. For example, do not engage in defamation (harming another's reputation by lies); do not employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; do not upload a work, virus, trojan horse, time bomb, or other harmful form of programming or vandalism; do not participate in hacking activities or any form of unauthorized access to other computers, networks, or information systems.

b) Uses that jeopardize the security of student access and of the computer network or other networks on the Internet are prohibited. For example, do not disclose or share your password with others; do not impersonate another user.

c) Uses that are commercial transactions are not allowed. Students may not use the SCS or school network to sell or buy anything over the Internet. You should not give others private information about yourself or others.

d) Illegal activities, including copyright or contract violations, shall not be permitted on the Internet.

e) The Internet shall not be used for commercial, political, illegal, financial, or religious purposes. Violations shall be reported to a teacher or an administrator immediately.

f) Threatening, profane, harassing, or abusive language shall be forbidden.

g) Use of the network for any illegal activities is prohibited. Illegal activities include (a) tampering with computer hardware or software, (b) unauthorized entry into computers and files (hacking), (c) knowledgeable vandalism or destruction of equipment, and (d) deletion of computer files. Such activity is considered a crime under state and federal law. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

h) No user is permitted to knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system. No third party software will be installed without the consent of the assigned administrator.

i) Invading the privacy of another user, using another's account, posting personal messages without the author's consent, and sending or posting anonymous messages shall be forbidden.

j) Accessing pornographic or obscene materials or using or sending profanity in messages is forbidden.

k) Any subscription to list serves, bulletin boards, or on-line services shall be approved by the superintendent or his designee prior to any such usage.

l) The use of anonymous proxies or any site that allows the user to get around content filtering is strictly prohibited and is a direct violation of this agreement.

Internet Safety

- Parents and Users: Despite every effort for supervision and filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.

Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

- Personal Safety: In using the network and Internet, users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet.
- Confidentiality of Student Information: Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.
- Active Restriction Measures: The District will utilize filtering software or other technologies to prevent all users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The filter can be disabled for adults engaged in bona fide research or for other lawful purposes. The use of anonymous proxies or any site that allows the user to get around the content filter is strictly prohibited and will be considered a violation of this policy. All teachers will use due diligence to monitor minors while on the Internet, and faculty and staff will encourage students to be safe online.
- All minors should be educated each year about appropriate online behavior, including cyberbulling, awareness and response, and interacting with other individuals on social networking sites and in chat rooms.

Use of New Web Tools

Online communication is critical to our students' learning of 21st Century Skills. Tools such as blogging and podcasting offer authentic, real-world vehicles for student expression. Again, as educators, our primary responsibility to students is their safety. Hence, expectations for classroom blogs, student protected e-mails, podcasts, or other Web interactive use must follow all established Internet safety guidelines.

Blogging/Podcasting Terms and Conditions:

- The use of blogs, podcasts or other Web 2.0 tools is considered an extension of your classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other Web 2.0 tools. This includes, but is not limited to, profanity and racist, sexist or discriminatory remarks.
- Teachers must monitor all communication on blogs, podcasts, or other Web 2.0 tools that are used in the classroom.
- Students using blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their posts.
- A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including addresses or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
- Any personal blog a student creates in class is directly linked to the class blog which is typically linked to the student profile, and, therefore, must follow these blogging guidelines. In addition to following the information above about not sharing too much personal information (in the profile or in any posts/comments made), students need to realize that anywhere they use their blog login it links back to the class blog. Therefore, anywhere that login is used (posting to a separate personal blog, commenting on someone else's blog, etc.), the account should be treated the same as a school blog and should follow district blogging guidelines. Comments made on blogs should be monitored and - if they are inappropriate – deleted.
- Never create a link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.
- Students using Web 2.0 tools agree to not share their user name or password with anyone besides their teachers and parents and to treat blogspaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

Teacher Responsibilities

- Provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the district curriculum
- Inform all students of their rights and responsibilities as users of the district network prior to gaining access to that network, either as an individual user or as a member of a class or group
- Use networked resources in support of educational goals
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy
- Provide alternate activities for students who do not have permission to use the internet
- To comply with CIPA, teachers must educate minors about appropriate online behavior, interacting with other individuals on social networking websites and in chat rooms and cyber-bulling awareness and response.
- All teachers will use due diligence to monitor minors while on the Internet, and faculty and staff will encourage students to be safe online.

Principal Responsibilities

- Include Acceptable Use Policy in student handbook
- Be sure handbooks are distributed to all students
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy
- Keep permission forms on file for one year
- Identify students who do not have permission to use the internet to the teaching staff
- To comply with CIPA, principals must educate all faculty and staff about appropriate online behavior, interacting with other individuals on social networking websites and in chat rooms and cyber-bulling awareness and response.
- Insure that teachers are educating students about appropriate online behavior about appropriate online behavior, interacting with other individuals on social networking websites and in chat rooms and cyber-bulling awareness and response.
- Insure that all teachers will use due diligence to monitor minors while on the Internet and when using Gaggle email, and insure that faculty and staff will encourage students to be safe online.

District Responsibilities

- Ensure that filtering software is in use to block access to materials that are inappropriate, offensive, obscene, or contain pornography.
- Have Acceptable Use Policy approved by the board and reviewed yearly.
- Monitor network use and filtering for inappropriate activities by users according to the district Internet Monitoring Policy.

Union Parish School Board
Acceptable Use Policy and Internet Safety
Consent Form

As a parent or legal guardian of _____ I have read and understand the Acceptable Use Policy, and I agree to the following:

(Please initial where appropriate)

_____ As the parent or legal guardian of the student named above, I grant permission for my son or daughter to use a school computer or network software provided by the Union Parish School Board.

_____ As the parent or legal guardian of the student named above, I grant permission for my son or daughter to access Internet services provided by the Union Parish School Board.

_____ As a parent or legal guardian or the student named above, I grant permission for my son or daughter's photo, without identifying name or caption, to appear on any district, school, or teacher website connected with the Union Parish School Board.

_____ As a parent or legal guardian or the student named above, I grant permission for my son or daughter's school work to be published without identifying name or caption, to appear on any district, school, or teacher website connected with the Union Parish School Board.

Childs Name (Please Print): _____

Childs School: _____

Parent phone number: _____

Parent email address: _____

Student Signature: _____

Parent (Guardian) Signature: _____