

**Page County Public Schools
Acceptable Use Policy
and
Internet Safety Program**

March 2009

Legislation approved by the 2006 General Assembly and signed by Governor Kaine requires the addition of a student Internet safety component to division Acceptable Use Policies (AUP).

The legislation requires Internet safety to be integrated within each school division's academic instructional program. It also directs the Superintendent of Public Instruction to issue guidelines regarding Internet safety instruction.

The pages that follow addresses:

- ✓ Acceptable Use Policy (code requirement)
- ✓ Internet Safety Program (program requirement)
- ✓ Acceptable Use Policy – Student Statement of Acceptance – Appendix A
- ✓ Acceptable Use Policy – Parental Permission for Student – Appendix B
- ✓ Acceptable Use Policy – All School Personnel Statement of Acceptance
Appendix C

Note: Once approved this document must be submitted to VDOE by July 1, 2009. This document must be made available in electronic format. Will it be the Board's pleasure to have this document placed on the county's web page?

**Page County Public Schools
Acceptable Use Policy
March 2009**

A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy (AUP), approved by the local school board, for the Internet.

Every two years, the acceptable use policy will be reviewed and revised as necessary then presented to the division superintendent and school board for approval. After the policy receives approval, the Division Superintendent will file the revised Acceptable Use Policy for the Internet with the Superintendent of Public Instruction.

At a minimum, the policy shall contain provisions that (i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet.

At a minimum, the policy shall contain provisions that (ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in §18.2372.

At a minimum, the policy shall contain provisions that (iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in §18.2-374.1:1 and obscenity as defined in §18.2-372.

Filtering System

The computer equipment and communication services are first protected by the WatchGuard firewall. This appliance protects the networking system from viruses, hackers, and potentially harmful .exe files. Requests that are deemed acceptable by the firewall must pass through a second filtering system.

Our school division utilizes an Internet filtering system known as Iprism/St. Bernard. This appliance and software works to prohibit the user of computer equipment and communications services from sending, receiving, viewing, or downloading illegal/inappropriate material via the Internet. All Internet traffic generated by computer requests must pass through this filtering system to determine acceptable access. If the requested information is determined to be unacceptable the user requesting the information will receive an access denied screen. The user can then see why the request was denied. In order to filter or block Internet access to child pornography as set in §18.2-374.1:1 and obscenity as defined in §18.2-372 and any other inappropriate materials as defined in §18.2372, the parameters of the filtering system are set up to deny access to requests involving information that is included in the following categories:

Sex: adult, nudity, sexuality, lingerie/bikini, pornography;
Questionable Activities: computer hacking, miscellaneous questionable, tasteless, weapons/bombs, intolerance/extremism, profanity, violence, copyright infringement;
Malware: malware, phishing, spyware/adware;

Society: cult

Internet: high bandwidth, online chat, sharewares download, web host, email host

Business: online auctions

Recreation: games, mature humor, gambling, digital music

This system also allows the manual blocking of sites deemed to be inappropriate for the educational setting. Any school personnel can request sites to be blocked by supplying solid reason(s) why the site(s) should be deemed inappropriate.

Communication Services

Our school division limits communication services via email to adult school employees only. Students are not given accounts for the Ipswitch Imail system and other email systems/services are blocked by the filtering system. The Ipswitch system restricts attachments deemed to be potentially harmful. There is also an anti-spam filter that separates email identified as spam from non-harmful emails. The communication service of instant messaging is currently prohibited for student use.

Disclaimer

With all filtering appliances and software resources working properly, occasionally (because of new web sites that have not had sufficient time to be rated) Internet users are able to access inappropriate material. Close monitoring by all employees is required in order to detect and report the viewing of such materials.

Additional Page County Public Schools Computer and Internet Use Policy

Acceptable Uses

- School technologies are for the educational use of students and faculty. Student uses of computers are to be limited to activities that reinforce/enhance the essential skills as stated in the *Virginia Standards of Learning* and/or objectives of classroom instruction.
- The primary use of the Internet is for research and inquiry that enhances student learning. The playing of games that do not support the learning of essential skills, visiting chat rooms, instant messaging, downloading files, playing music, and streaming non-curriculum related videos are not allowed.
- Collaboration/communication tools such as blogs, student emails, wikis, forums, and other Web 2.0 tools can be used only if the following guidelines are adhered to:
 1. use of such tools must be for a specific teacher-driven educational activity
 2. the specific teacher-driven educational activity must have prior approval of the building principal
 3. teachers must monitor the content of student communications (the security of the tool must be capable of providing a method of monitoring all communications)

4. at the conclusion of a project it is the responsibility of the teacher to stop all access to the communication feature of the tool.
 5. the establishing of student accounts must be done in a manner that protects the identity of the student (student's names cannot be used as identifiers)
- Vandalism is NOT acceptable and will not be tolerated. Vandalism is defined as any malicious attempt to harm or destroy equipment and/or data, including, but not limited to: uploading, creating, or transmitting computer viruses, tampering with computer programs, and changing or deleting files other than your own. Such behavior could result in cancellation of user privileges and disciplinary action.
 - Acts or attempted acts to bypass the security/filtering system will NOT be tolerated. The use of proxy or proxy-like applications that allow unfiltered access to Internet materials by teachers or students is in direct violation of state and division policies. Such behavior could result in cancellation of user privileges and disciplinary action.

Rights and Responsibilities

- Access is a privilege, not a right; students and faculty are responsible for their use of the Internet. The use of the Internet should be for the purpose of education and research and must be consistent with the educational goals of Page County Public Schools.
- Students and faculty must comply with all school, local, state, and federal laws including those regarding the transmission of copyrighted, threatening, or obscene material. In addition, the Internet may **NOT** be used for commercial activities, product promotion, political lobbying (unless a component of a teacher-driven project), or illegal activities.
- Student access to the Internet must be under the supervision of instructional faculty and staff members. Students must not access the Internet if school personnel are not monitoring their activities. Students that come upon inappropriate materials are required to turn off the computer monitor and report inappropriate findings to the adult monitor in the room. The adult receiving this information must note the URL of the inappropriate material and report this immediately to the building principal and technology staff who will block any future viewing of the material.
- Network drives should not be considered private. School personnel have access to all files. Files relating to or in support of illegal activities or conflicting with school policies will be reported to the authorities, and disciplinary actions will follow.
- Students and faculty must respect copyrights and give appropriate credit.
- As stated in the *Page County Public Schools Student Code of Conduct and Attendance*: “any type of electronic or mechanical device which distracts or impedes the educational process is prohibited”. This includes but is not limited to personal laptops and other Internet accessible devices which are prohibited without prior permission of building administrator.

Policy for Web Publication:

Web pages offer another tool to increase communication between home and school. Teachers are encouraged to create web pages for use with their classes. Teacher web pages containing any school related information can only be posted on one of the following websites:

- Quia
- TeacherWeb
- other division supported web sites
- Page County Public School web server

The following policy must be followed when creating a web site or pages:

- Any web page must be created in a professional manner and cannot contain any negative connotations.
- Before publishing any picture or name of a student, it is the responsibility of the person creating the web page to verify the existence of a signed permission from the parent giving consent for the release of this information. Record of this consent can be obtained from the child’s homeroom teacher or school office. If record of this consent cannot be located, the responsibility of obtaining such consent becomes the responsibility of the web page creator before publication.
- Pictures of students may be used but **NO** individual student name can be displayed with the picture or in the context of the web page. Pictures can be identified by group name only (ex. 2nd grade field trip).
- Student names may be used as long as there are **NO** associated pictures (ex. Science fair winners can be listed but no picture of the winners may be present on the web site).
- **A web site can contain pictures or names but cannot contain both.**
- It is the responsibility of the person creating the web page to have the completed project viewed by the building principal and obtain his/her permission for publishing.
- **At a minimum, the policy shall contain provisions that (iv) establish appropriate measures to be taken against persons who violate the policy.**

Violations by Student:

The violation of any portion of the policy by student(s) must be reported to the building principal or assistant principal. Violations could result in cancellation of user privileges and disciplinary action. If the student is found in violation of State or Federal laws, a referral will be made to the local authorities.

Violations by Staff:

Any staff member found to be in violation of any portion of this policy, including the failure to properly supervise students using computers, shall be notified of their violation by the building supervisor. If any staff member is found in violation of State or Federal laws, a referral will be made to the local authorities.

The policy may include such other terms, conditions, and requirements as deemed appropriate, such as requiring written parental authorization for Internet use by juveniles or differentiating acceptable uses among elementary, middle and high school students.

Page County Public Schools requires parents, students and staff to read, review and sign the Acceptable Use Policy at the beginning of each school year. Any person failing to sign the policy, therefore, establishing no commitment to abide by the policy, is denied use of any computer equipment that runs software or has Internet access.

The superintendent shall take steps as he deems appropriate to implement and enforce the division's policy.

Technology is an integral part of Page County Public Schools daily instruction. I (Dr. Randall W. Thomas) am committed to enforcing this Acceptable Internet Use Policy to the fullest in order to help guarantee the safety of all of our students and staff.

**Page County Public Schools
Internet Safety Program
September 2008**

The AUP Internet safety program contains a descriptive statement(s) regarding the division's instructional philosophies and strategies to be supported by Internet access in schools.

Page County Public Schools use a variety of educational technologies to enhance student learning. The use of Internet resources is viewed by this school division as an integral part of daily classroom instruction. We support this philosophy by providing access to the Internet in all instructional settings (classrooms, libraries, computer labs, etc...) in our division. The division encourages the integration of these valuable resources into the teaching and learning environment by providing training opportunities to teachers.

The AUP Internet safety program specifies the roles and responsibilities for division personnel (including but not limited to administrators, teachers, counselors, instructional technology resource teachers, library media specialists, building resource officers, and information technology coordinators) and students with regard to the acceptable use of electronic based resources and Internet safety. An overview and outline of the program is available in electronic format for all to view.

Page County Public Schools view the use of the Internet as a privilege, not a right. Therefore, all division personnel and students are responsible of knowing and using safe practices while engaged in computer/Internet use. All division personnel must accept the guidelines set forth in the division's *Internet Acceptable Use Policy: All School Personnel Statement of Acceptance* (Appendix C). In order for a student to be given Internet access privileges, his or her parent/guardian must first grant permission by agreeing to and signing the *Internet Acceptable Use Policy: Parent Permission for Student* (Appendix B). Second, the student must sign the *Internet Acceptable Use Policy for Students* (Appendix A), thus showing their agreement to abide by the policies stated. All three policies can be viewed in electronic format.

Specific roles and responsibilities of administrators: The roles of the administrators (central office and building) are to assist in the development and/or revision of the Acceptable Use Policy. Personnel serving in an administrator position are responsible for enforcing the Acceptable Use Policy and taking the necessary actions when violations of the policy occur.

Specific roles and responsibilities of instructional personnel: The role of instructional personnel is to monitor student use of electronic resources and Internet Safety on a daily basis. Personnel serving in these positions are responsible for abiding by, reinforcing, and reporting violations of the policy. Each school year all instructional personnel must implement a plan for integrating Internet Safety into their curriculum. This plan must include documentation of four occurrences in which Internet Safety was integrated into the classroom instruction.

Specific roles and responsibilities of building resource officers: The role of the building resource officer is to serve as a resource for the teaching and practices of Internet Safety. Personnel serving in this position

shall assist the administration and instructional personnel by providing information about current Internet activity that could have a negative impact on students. These individuals may be used to assist school administration in investigating and dealing with violations of the Acceptable Use Policy, vandalism to hardware, and actions by students or employees that have the potential to compromise the integrity of the networking system.

Specific roles and responsibilities of information technology coordinators: The role of the information technology coordinators is to be a resource to the administrator, instructional personnel, and students. Personnel serving in this position shall be responsible for making revision suggestions to the Acceptable Use Policy and Internet Safety Program. These coordinators shall provide training to instructional personnel in an effort to keep all personnel informed of changes in digital resources and Internet Safety. Coordinators shall assist instructional personnel in their efforts to enhance their daily instruction through the use of technology resources.

The AUP Internet safety program specifies roles and responsibilities for community stakeholders with regard to the acceptable use of electronic-based resources and Internet safety.

Specific roles and responsibilities of community stakeholders: The role of the community stakeholders is to be informed about the use and abuse of digital media. The stakeholders have the responsibilities to be aware of the inappropriate content and threats that digital media presents to the children of the community. In each household where there is access to digital media, stakeholders should obtain a level of knowledge that will enable them to protectively monitor the use of such resources by minors in their care. The school community shall assist them in obtaining this knowledge by working with PTAs/PTOs, providing printed media, and maintaining an Internet Safety website that is accessible to the community stakeholders.

The AUP Internet safety program specifies safety measures in place, including filtering and monitoring procedures. The plan identifies measures for future implementation.

Page County Public Schools strives to address issues of concern that threaten the safety of people and equipment. The computer equipment and communication services are first protected by the WatchGuard firewall. This appliance protects the networking system from viruses, hackers, and potentially harmful files. Requests that are deemed acceptable by the firewall then pass through a filtering system known as Iprism/St. Bernard. This appliance and software works to prohibit the users of computer equipment and communication services from sending, receiving, viewing, or downloading illegal/inappropriate material (pornography, obscenity, etc...) via the Internet.

In order to maintain the highest level of safety from emerging inappropriate Internet content, our school division constantly monitors and makes adjustments in the structure of the filtering system. The appliances and software are updated on a scheduled basis to provide the computer user the most protection possible while allowing access to materials that can be used to enhance instruction. Even with multiple levels of security, applications that can be used to bypass the filtering system are found and used by individuals. Monitoring of the Iprism by the technology director is conducted frequently to search for use of such applications. When found much effort and attention is given to preventing its recurrence.

Access to Internet content that utilizes excessive bandwidth is limited to after school viewing and downloading in order to maintain the necessary bandwidth needed for instructional and productivity activities.

The Acceptable Use Policy is a living document. Changes are made to the policies in order to provide guidelines and acceptable use of emerging technologies.

The AUP Internet safety program describes methods by which the division ensures data and network security. The division’s policy should correlate with local Continuity of Operations Plan (COOP).

Page County Public Schools strives to ensure data and network security by incorporating the following:

1. Access to sensitive data is controlled by password access. This access is limited to only the school personnel who are responsible for maintaining the data.
2. Passwords are changed immediately if there is any suspicion their integrity has been compromised.
3. Firewall is maintained to ensure that the network is not compromised by hackers and other with the intent to do harm.
4. Data that is saved to the servers in each building is backed-up on a daily basis to a tape backup. At any given time data can be restored up to five weeks.
5. Student Information System is backed-up to an off-site location and locally to tape on a nightly basis.

The AUP Internet safety program describes technology-based applications and hardware prohibited for employee and student use. It identifies associated penalties.

Students and division personnel must comply with all school, local, state, and federal laws including those regarding the transmission of copyrighted, threatening, or obscene material. Applications that serve to bypass the filtering system are strongly prohibited. In addition, the Internet may NOT be used for commercial activities, product promotion, political lobbying (unless a component of a teacher-driven project), or illegal activities. Any user violating these provisions, state or federal laws, classroom or school district rules, is subject to loss of Internet privileges and other student and faculty disciplinary actions, including criminal prosecution.

The AUP Internet safety program describes procedures to address breaches of Internet and intranet security and safety. Legal actions resulting from breaches have been reviewed.

Violations by Student:

The violation of any portion of the Acceptable Use Policy by student(s) must be reported to the building principal or assistant principal. If the student is found in violation of State or Federal laws, a referral will be made to the local authorities.

Violations by Staff:

Any staff found to be in violation of any portion of the Acceptable Use Policy, including the failure to properly supervise students using computers or the use of applications for the purpose of bypassing the filtering system, shall be notified of their violation by the building supervisor. If any staff member is found in violation of State or Federal laws, a referral will be made to the local authorities.

The AUP Internet safety program describes ongoing professional development opportunities for each stakeholder group. It includes an overview of both the needs assessment and evaluation processes for professional development and community outreach programs.

Page County Public Schools plans ongoing Internet Safety training opportunities for school personnel and the community. The professional development opportunities for school personnel will be changing as the use and misuse change but will be delivered through the following avenues:

- Personnel serving as Instructional Technology Resource Teachers will provide training or informational sessions as requested or deemed necessary on topics dealing with Internet Safety. As a result of the needs assessment conducted in May 2008 session topics will include but not limited to:
 - Specific ways to integrate Internet Safety into any instructional setting
 - Examining the Internet Safety resources and their potential usages
 - Internet Awareness – search engines, spyware, malware, viruses, pop-ups, domain extension, download files, advertisements, etc...
 - Web 2.0 tools and security practices while utilizing these tools
 - Cyber Bullying
 - Social Networking
- The school division will seek out and utilize outside resources from other state organizations and professionals that specialize in Internet Safety.

An evaluation and needs assessment of the Internet Safety Program shall be delivered in the form of an online survey at the end of each school session. This survey will be completed by all instructional personnel. The information obtained from this survey will be used to make adjustments in the Internet Safety Program.

Page County Public Schools are committed to assisting the community stakeholders in obtaining knowledge about the use and abuse of the Internet and other digital media. The school community shall participate in a community outreach program to assist stakeholders in obtaining the knowledge necessary to be informed Internet users. It is the school division's desire to work with PTAs/PTOs to share knowledge and to serve as a resource to the community. The division will provide printed media, and maintain an Internet Safety website that is accessible to the community stakeholders.

At the end of the school session, an evaluation and needs assessment of the Internet Safety Program shall be requested of members of the participating PTAs/PTOs. This evaluation/assessment shall be delivered through paper-pencil or online. The information obtained from this survey will be used to make adjustments in the Internet Safety Program.

The AUP Internet safety program describes community outreach activities that are consistent with the program's goals. It includes an overview of both the needs assessment and evaluation processes for community outreach programs.

Page County Public Schools are committed to assisting the community stakeholders in obtaining knowledge about the use and abuse of the Internet and other digital media. The school community shall participate in a community outreach program to assist stakeholders in obtaining the knowledge necessary to be informed Internet users.

In November, 2007, the school division and the Page County Sheriff's Department co-sponsored an informative meeting for the Page County community. The meeting was held in a central location within the county to encourage greater participation. This attempt to inform the public met with limited participation. In October/November of 2008, the elementary schools held a Literacy Night in which information on Internet Safety was offered. Therefore, it is the school division's desire to work with PTAs/PTOs to share knowledge and to serve as a resource to the community. The division will provide printed media, such as Internet Safety tips, safe use guidelines and personal safety goals in school newsletters. Division personnel will continue to maintain an Internet Safety website that is accessible to the community stakeholders. This website will serve as a resource for community members searching for such information.

At the end of the school session, an evaluation and needs assessment of the Internet Safety Program shall be requested of members of the participating PTAs/PTOs. This evaluation/assessment shall be delivered through paper-pencil or online. The information obtained from this survey will be used to make adjustments in the Internet Safety Program.

The AUP Internet safety program describes the division's procedures for the evaluation and revision of the AUP, including the Internet safety program.

Following the 2007-2008 implementation year division teachers completed an online survey regarding their perspective on the Internet Safety program, their proficiency with Internet Safety integration and what they would like to see changed about the program. These perspectives were utilized to revise the Internet Safety program to better meet the needs of both the teachers and the students. This procedure for evaluation and gathering information will take place at the end of each school year. To address the needs of all stakeholders and the ever-changing advancement in technology, the Acceptable Use Policy and the Internet Safety Program will be reviewed by June 30 of each year.

The AUP and Internet safety program have been implemented, enforced, evaluated, and adjusted when needed.

By September 2008, Page County Public Schools Acceptable Use Policy and Internet Safety Program will have been presented to the School Board. If needed, adjustments will have been made in order to meet the School Board's approval.

The Internet Safety Program was developed in the latter part of the 2006 -07 school year. During the 2007-08 school year, the program was implemented for the first time. The program has been evaluated and revised for the 2008-09 school year.

The Acceptable Use Policy is reviewed annually and revised to address issues and concerns that directly impact the use of Internet resources to enhance the daily instructional setting.

Page County Public Schools

Internet Acceptable Use Policy Student Statement of Acceptance Revised - March 2009

Page County Schools use a variety of educational technologies to enhance student learning. Use of the Internet, which is a worldwide network of computers linked to each other, can provide unique educational resources for student research and learning. Internet resources can change the way in which students access information and can provide a wealth of information for research and inquiry. The ability to gain access to an unlimited amount of data is an invaluable benefit for students. Access to the Internet for students is a **privilege** provided in libraries, computer labs, and classrooms in our county schools.

Students are responsible for good behavior on school computer networks, just as they are in a classroom or school hallway. In order for a student to be given Internet access privileges, his or her parent/guardian must first grant permission by agreeing to and signing the **Parent Permission Form**. Second, the student must sign this **Internet Acceptable Use Policy for Students** thus showing their agreement to abide by the policies stated.

Acceptable Uses

- School technologies are for the educational use of students. Student uses of computers are to be limited to activities that reinforce/enhance the essential skills as stated in the *Virginia Standards of Learning* and/or objectives of classroom instruction.
- The primary use of the Internet is for research and inquiry that enhances student learning. **The playing of games that do not support the learning of essential skills, visiting chat rooms, instant messaging, downloading files, playing music, student email (unless a component of a teacher-driven project), and streaming non-curriculum related videos are not allowed.**
- Vandalism is **NOT** acceptable and will not be tolerated. Vandalism is defined as any malicious attempt to harm or destroy equipment and/or data, including, but not limited to: uploading, creating, or transmitting computer viruses, tampering with computer programs, and changing or deleting files other than your own. Such behavior may result in cancellation of user privileges **and** disciplinary action.

Access Restrictions

Page County Schools utilizes software that provides Internet control, monitoring and filtering. This software is critical since it allows valuable on-line Internet access while restricting access to specific unwanted categories including pornography, gambling, illegal drugs, criminal skills, games, etc. However, occasionally Internet users are able to access inappropriate material. In such instances, the student is required to immediately close out of the inappropriate site and report this finding to the closest school staff.

Students can also gain access to inappropriate, non-educational websites by the use of a proxy or proxy-like application that allows unfiltered access by bypassing the security/filtering system. Using, attempting to use or searching for such applications by students (and all school personnel) will not be tolerated.

Student Statement of Acceptance Continued

Rights and Responsibilities

- Access is a privilege, not a right; students are responsible for their use of the Internet. The use of the Internet should be for the purpose of education and research and must be consistent with the educational goals of Page County Schools.
- Students must comply with all school, local, state, and federal laws including those regarding the transmission of copyrighted, threatening, or obscene material. In addition, the Internet may **NOT** be used for commercial activities, product promotion, political lobbying (unless a component of a teacher-driven project), or illegal activities.
- Student access to the Internet must be under the supervision of instructional faculty and staff members. Students must not access the Internet if school personnel are not monitoring their activities.
- Network drives are created to allow students and instructional personnel a place to save materials in a convenient and quick manner. These shared drives should not be considered private but **NO** student has the right to delete or modify another person's saved materials. The deleting/modifying of any files other than your own will be viewed as stealing/destroying/defacing of property. Files containing content in support of illegal activities or conflicting with school policies will be reported to the authorities, and disciplinary actions will follow.
- Students must respect copyrights and give appropriate credit.
- As stated in the *Page County Public Schools Student Code of Conduct and Attendance*: "any type of electronic or mechanical device which distracts or impedes the educational process is prohibited". This includes but is not limited to personal laptops and other Internet accessible devices which are prohibited without prior permission of building administrator.
- **Any user violating these provisions, state or federal laws, classroom or school district rules, is subject to loss of Internet privileges and other student disciplinary actions, including criminal prosecution.**

Network Etiquette

- Be polite, courteous, and respectful in all network activities; rudeness is unacceptable.
- Use appropriate language; do not use profanity, vulgarities or other abusive or inappropriate language.
- Transmission of obscene materials is prohibited. Users who inadvertently access information that is objectionable should report any such activity to the supervising teacher immediately.
- Do not reveal your personal address and phone number or those of other students.
- Do not share your password or use another person's password.

I have read and understand my responsibilities as outlined in this policy. I agreed to abide by all regulations outlined above. I understand that my failure to do so will result in loss of privileges and disciplinary actions.

Student Name (please print)

Student Signature

Date

Page County Public Schools

**Internet Acceptable Use Policy
Parental Permission for Student
Revised – March 2009**

Page County Schools use a variety of educational technologies to enhance student learning. Use of the Internet, which is a worldwide network of computers linked to each other, can provide unique educational resources for student research and learning. Web based educational programs to which the county subscribes are an integral part of daily instruction. Internet resources can change the way in which students access information and can provide a wealth of information for research and inquiry. Access to the Internet for students is a **privilege** provided in libraries, computer labs, and classrooms in our county schools.

The ability to gain access to an unlimited amount of data is an invaluable benefit for students. However, on a global network it is impossible to control all materials. Ultimately, school staff, parents and guardians of minors are responsible for setting and conveying the standards that students should follow when using media and information sources. Staff members will make every effort to ensure that student use of the Internet is appropriate and educational.

Page County Schools utilizes software that provides Internet control, monitoring and filtering. This software is critical since it allows valuable on-line Internet access while restricting access to specific unwanted categories including pornography, gambling, illegal drugs, criminal skills, and games. However, occasionally Internet users are able to access inappropriate material. In such instances, the school system expects the students to immediately close out of the inappropriate site and report this finding to the closest school staff. Students can also gain access to inappropriate, non-educational websites by the use of a proxy or proxy-like application that allows unfiltered access by bypassing the security/filtering system. Using, attempting to use or searching for such applications by students (and all school personnel) will not be tolerated.

If parents grant permission for their child to use the Internet, the child will be informed of his/her responsibilities and be required to sign a form agreeing to abide by stated rules and regulations (Student Acceptable Use Policy) before Internet access will be granted. **Any user violating these provisions, state or federal laws, classroom or school district rules, is subject to loss of Internet privileges and other student disciplinary actions, including criminal prosecution.**

Page County Schools support and respect the rights of parent(s) or guardian(s) to decide whether or not to allow their child access to the Internet.

-----Cut here and return the bottom portion to school personnel-----

<input type="checkbox"/> Do	give permission for my child to have access to the Internet. I understand that my child must follow school guidelines while on the Internet to keep these privileges.
<input type="checkbox"/> Do NOT	give permission for my child to have access to the Internet.

Child's Name (please print)

Signature of Parent / Guardian

Date

Page County Public Schools

Internet Acceptable Use Policy All School Personnel Statement of Acceptance Revised – March 2009

All school personnel in Page County Public Schools have access to a variety of educational technologies that can be used to enhance instruction and improve student learning. The Internet and the vast resource it provides can allow for reinforcing and enriching educational experiences as well as the opportunity for collaborative work.

Access to the Internet for all school personnel use is a **privilege** provided in libraries, computer labs, and classrooms in the county schools. However, on a global network it is impossible to control all materials. **Ultimately, all school personnel, parents and guardians of minors are responsible for setting and conveying the standards that students should follow when using media and information sources.** Staff members must make every effort to ensure that student use of the Internet is appropriate and educational.

Acceptable Uses

- School technologies are for the educational and administrative use of school personnel and students. Computer activities are to be planned by the teacher to reinforce classroom instruction, essential skills, or other educational purposes.
- The primary use of the Internet is for research and inquiry that enhances teacher instruction and student learning. **The playing of games that do not support the teaching of essential skills, visiting chat rooms, instant messaging, downloading files, playing music, and streaming non-curriculum related videos are not allowed.**
- All students are allowed to view Internet sites that are projected from one computer by the teacher for instructional purposes. This is the only time that students may view online Internet sites without a signed **Parent Permission Form** and **Student Internet Use Agreement** on file.
- Collaboration/communication tools such as blogs, student emails, wikis, forums, and other Web 2.0 tools can be used only if the following guidelines are adhered to:
 1. use of such tools must be for a specific teacher-driven educational activity
 2. the specific teacher-driven educational activity must have prior approval of the building principal.
 3. teachers must monitor the content of student communications (the security of the tool must be capable of providing a method of monitoring all communications)
 4. at the conclusion of a project, it is the responsibility of the teacher to stop all access to the communication feature of the tool.
 5. the establishing of student accounts must be done in a manner that protects the identity of the student (student's full names cannot be used as identifiers)

- Web pages offer another tool to increase communication between home and school. Teachers are encouraged to create web pages for use with their classes. Teacher web pages containing any school related information can only be posted on one of the following websites:
 - Quia
 - TeacherWeb
 - other division supported web sites
 - Page County Public School web server

The following policy must be followed when creating a web site or pages:

- Any web page must be created in a professional manner and cannot contain any negative connotations.
- Before publishing any picture or name of a student, it is the responsibility of the person creating the web page to verify the existence of a signed permission from the parent giving consent for the release of this information. Record of this consent can be obtained from the child’s homeroom teacher or school office. If record of this consent cannot be located, the responsibility of obtaining such consent becomes the responsibility of the web page creator before publication.
- Pictures of students may be used but **NO** individual student name can be displayed with the picture or in the context of the web page. Pictures can be identified by group name only (ex. 2nd grade field trip).
- Student names may be used as long as there are **NO** associated pictures (ex. Science fair winners can be listed but no picture of the winners may be present on the web site).
- **A web site can contain pictures or names but cannot contain both.**
- It is the responsibility of the person creating the web page to have the completed project viewed by the building principal and obtain his/her permission for publishing.

Rights and Responsibilities

- It is the responsibilities of all staff members to, at all times, closely monitor the student use of the Internet and other computer activities. ***At no time should a student be using a computer without close monitoring by school personnel. The close monitoring of students requires the supervising adult to make direct eye contact with the screens of the computers being used by the students. This level of supervision and the positioning of computers will require the supervising adult to frequently circulate among the computer users.***
- It is the responsibility of any school personnel who observes a student engaging in any of the following activities to stop the activity and refer the student to the school administration: the playing of games that do not reinforce essential skills, visiting chat rooms, instant messaging, downloading files, playing music, student email (that is not a part of a teacher-driven project), streaming non-curriculum related videos, and the viewing of material that is deemed as inappropriate by the supervising adult.

All School Personnel Statement of Acceptance Continued

- At any location where students can/are accessing the Internet, it is the responsibility of school staff to verify that the student(s) using the Internet has a Parent Permission Form and Student Internet Use Agreement on file allowing such access.
- If parents have not given permission for their child to access the Internet, the supervising adult cannot allow the student access to the Internet. If a teacher makes an assignment that requires the use of the Internet, an equivalent, alternate assignment must be given to the student.
- Internet websites that are integrated into a teacher's instruction must be thoroughly previewed prior to use with students. Sites that contain numerous pop-up advertisements must be avoided because they have a high potential of downloading harmful spyware to the computer.
- Page County Public Schools have a filtering system in place to block inappropriate web content; however, occasionally Internet users are able to access inappropriate material. If this occurs it is the responsibility of the supervising adult to note the web address, shut out of the web site, and notify the building principal and technology staff immediately so that the site can be blocked as soon as possible.
- Personnel must comply with all local, state, and federal laws regarding the transmission of copyrighted, threatening, or obscene material. In addition, the Internet may not be used for commercial activities, product promotion, political lobbying (unless a component of a teacher-driven project), or illegal activities.
- Any material posted for public access on the Internet must follow the *Policy for Web Publication*. This includes information listed in school or teacher web sites.
- Personnel must respect copyrights and give proper credit.
- Acts or attempted acts to bypass the security/filtering system will **NOT** be tolerated. The use of proxy or proxy-like applications that allow unfiltered access to Internet materials by teachers or students is in direct violation of state and division policies.
- Any staff member found to be in violation of any portion of the Acceptable Use Policy shall be notified of their violation by the building supervisor. If any staff member is found in violation of State or Federal laws, a referral will be made to the local authorities.
- **Any user violating these provisions, state or federal laws, classroom or school district rules, is subject to disciplinary actions, including criminal prosecution.**

I have read, understand, and accept my responsibilities as outlined in *Internet Acceptable Use Policy - All School Personnel Statement of Acceptance*.

**Printed Name of School
Personnel**

School Personnel Signature

Date