

# Pike County Joint Vocational School District

## Computer Network and Internet Acceptable Use Policy for Students

Freedom of expression is an inalienable human right and the foundation for self-government. Freedom of expression encompasses the right to freedom of speech and the corollary right to receive information. Such rights extend to minors as well as adults. Schools facilitate the exercise of these rights by providing access to information regardless of format or technology. In a free and democratic society, access to information is a fundamental right of citizenship.

In making decisions regarding student access to the Internet, the Pike County Joint Vocational School District considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the Internet enables students to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The District expects that faculty will blend thoughtful use of the Internet throughout the curriculum and will provide guidance and instruction to students in its use. As much as possible, access from school to Internet resources should be structured in ways which point students to those which have been evaluated prior to use. While students will be able to move beyond those resources to others that have not been previewed by staff, they shall be provided with guidelines and lists of resources particularly suited to learning objectives.

Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media.

Students utilizing District-provided Internet access must first have the permission of and must be supervised by the Pike County Joint Vocational School District's professional staff. Students utilizing school-provided Internet access are responsible for good behavior on-line just as they are in a classroom or other area of the school. The same general rules for behavior and communications apply.

The purpose of District-provided Internet access is to facilitate communications in support of research and education. To remain eligible as users, students' use must be in support of and consistent with the educational objectives of the Pike County Joint Vocational School District. Access is a privilege, not a right. Access entails responsibility.

This document shall constitute the School District's Computer Network and Internet Acceptable Use Policy for students ("Policy"), and applies to all students who use or access the Network. A copy of this Policy shall be provided to students and their parents. Any use of your account that violates these policies may result in your access being withdrawn and/or additional disciplinary action. Violations of these policies are considered violations of the Student Code of Conduct and may result in disciplinary action up to and including suspension, expulsion, and/or referral to law enforcement. The District reserves the right to seek reimbursement of expenses or damages arising from student violations of these policies.

### **1. Reporting Misuse of the Network**

In addition to following the terms of this Policy, you should report any misuse of the Network to an instructor or to a District administrator. Misuse means any violation of this policy, such as commercial use of these resources, criminal activity, inappropriate content of e-mail sent to you by someone, or any other use that is not included in this policy but has the intent or effect of harming another or another's property.

**2. *Term of the Permitted Use***

Access to the Network is a privilege, not a right, and as such it may be suspended or revoked by the School District at any time for any reason. The School District may also limit access depending on student and staff schedules, equipment availability, or other constraints.

**3. *Access***

Network resources are only for use by authorized users. Anonymous use is not permitted, and access may not be shared or transferred. Students are assigned user id's and passwords that are seven characters that are randomly generated. Students shall not share their passwords or otherwise allow anyone to gain unauthorized access to the Network or the Internet. If you think someone may know your password, tell an instructor or District administrator and it will be changed. A student is subject to disciplinary action for any violations of this Policy committed by someone else who, with the student's express or implied permission or through the student's negligence, accesses the Network with the student's password.

**4. *Purpose and Use***

The School District is providing you access to its Network primarily to support and enhance your educational experience. Uses that interfere with normal District business or violate District policies are strictly prohibited, as are uses for the purposes of engaging in or supporting any kind of business or other profit-making activity. If you have any doubt about whether a contemplated activity is permitted, you may consult with an instructor or District administrator to help you decide if a use is appropriate.

**5. *Netiquette***

All users must abide by the rules of Network etiquette. Among the uses and activities that violate Network etiquette and constitute a violation of this Policy are the following:

- (a) Using inappropriate language, including swearing, vulgarities or other language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory or threatening.
- (b) Using the Network to make, distribute or redistribute jokes, stories or other material that would violate this Policy or the District's harassment or discrimination policies, including material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, sexual orientation or other protected characteristics.
- (c) Forwarding or redistributing the private message of an e-mail sender to third parties or giving the sender's e-mail address to third parties without the permission of the sender.
- (d) Creating technical difficulties for others, such as sending e-mail attachments that are too large to be accommodated by the recipient's system.
- (e) Attempting to reach Internet sites blocked by the software on school computers or to "hack" into other accounts or restricted information.
- (f) Using the Network in a manner inconsistent with the expectations of the Pike County Joint Vocational School District conduct of students. When using the Network, students should remember that they are representing themselves and their school to others.
- (g) Students are expected to act in a responsible, ethical and legal manner in accordance with District policy, accepted rules of network etiquette, and federal and state laws.

**6. Unacceptable Uses**

Among the uses and activities that are known to be unacceptable and constitute a violation of this Policy are the following:

- (a) **Uses or activities that violate the law or District policy** or that encourage others to violate the law or District policy. Among such uses or activities are the following:
- (i) Offering for sale or use or soliciting the purchase or provision of any substance the possession or use of which is prohibited by law or District policy.
  - (ii) Creating, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene or pornographic materials.
  - (iii) Creating, copying, viewing, transmitting, downloading, or uploading any materials that include the design or information for the purposes of creating an explosive device, materials in furtherance of criminal activities or terrorist acts, threatening materials or any other materials that violate or encourage others to violate the law or District policy.
  - (iv) Unauthorized copying, modifying, intruding, or attempts to copy, modify or intrude, into the folders, files, data, work, Networks, passwords or computers of others, or intercepting communications intended for others.
  - (v) Copying, downloading, uploading or transmitting student information, other confidential information or trade secrets.
  - (vi) Downloading and saving music or images, unless given permission by an instructor.
  - (vii) Engaging in harassment, stalking, or other repetitive unwanted communication, or using the Internet in support of such activities
  - (viii) Engaging in or supporting any kind of business or other profit-making activity.
- (b) **Uses or activities that cause damage to property.** Among such uses or activities are the following:
- (i) Uploading, downloading, creating or transmitting a computer virus, worm, Trojan horse, "hacking" software or other harmful component or corrupted data, or vandalizing the property of another. Vandalism includes any attempt to hack, alter, harm, destroy or interfere with the normal operation of software, hardware, data of another user, other District Network resources, or the use of the District Network to do any of the same acts on the Internet or outside Networks.
  - (ii) Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Even if materials on the Network are not marked with the copyright symbol, you should assume that they are protected under copyright laws unless there is explicit permission on the materials to use them.
- (c) **Commercial uses.** At no time may the Network or the Internet be accessed (including sending e-mail) for purposes of engaging in or supporting any kind of business or other profit-making activity. You may not sell or buy anything over the Internet, and you may not solicit or advertise the sale of any goods or services (whether to one recipient or many, such as "junk e-mail").

- (d) **Uses or activities that are unrelated to legitimate District purposes.** Users may not, during the school day, access the Internet for purposes of personal shopping, buying or selling items, connecting with a personal web site or weblog that is not part of a class project, receiving or posting messages to web sites or blogs not part of a class project, participating in any type of gaming activity, engaging in social or hobby activities during class time, engaging in or supporting any kind of business or other profit-making activity, or for general recreational web browsing unless it is during non-class time. (*Examples:* Amazon, eBay, Expedia, Drudge Report, dating services, chat rooms, poker web sites, CNN, ESPN, Halo.)
- (e) **Using District e-mail.** Students may be provided with a District e-mail account for educational purposes only. The District retains all rights and ownership to such accounts. Use of District e-mail for non-educational purposes, such as for operation of private business enterprises, is strictly prohibited.
- (f) **Uses that degrade or disrupt the operation of the Network or that waste limited computer and printer supplies or telephone resources.** For example, do not waste toner or paper in printers, and do not send chain letters, even for non-commercial or apparently "harmless" purposes, as these, like "junk e-mail," use up limited Network capacity resources.
- (g) **Uses that mislead others** or violate the standards of academic or personal integrity, including but not limited to plagiarism, disseminating untrue information about individuals or groups, or using another's password or some other user identifier that makes message recipients believe that someone other than you is communicating or otherwise using the other's access to the Network.
- (h) **Political uses:** Creating, transmitting or downloading any materials that support or oppose the nomination or election of a candidate for public office or the passage of a levy or a bond issue. Additionally, users shall not solicit political contributions through the Network from any person or entity or conduct any type of campaign business.
- (i) **Installing hardware or downloading and installing software** without the prior consent of the District's Technology Coordinator. You may not move, repair, reconfigure, modify or attach any external devices to Network equipment, computers or systems. You shall not remove, alter or copy the District's software for your own personal use or for the use of others.
- (j) **Respecting Resource Limits.** Students will use the system only for educational and career development activities and limited, high-quality, self-discovery activities. Students will not run software on this network unless it is owned and licensed by the District.

## 7. ***Confidentiality***

The confidentiality of any information stored in, created, received or sent over the e-mail system or through Internet access cannot be assured. To the extent feasible, students should therefore avoid transmitting personal information over the e-mail system or through Internet access.

## 8. ***Privacy***

Network access is provided as a tool for educational uses. 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 Network and any and all materials, files, information, software, communications (including emails) and other content transmitted, received or stored in connection with this usage. All such information, content and files shall be and remain the property of the District and you should not have any expectation of privacy regarding those materials. The Technology Coordinator or school administrators may review files and intercept communications for any reason, including but not limited to purposes of maintaining system integrity and ensuring that users are complying with this policy.

**9. *Entertainment Sites (Social Networking and Gaming Sites)***

Students may use the computer system only for legitimate educational purposes, which include classroom and independent research that is similar to the subjects studied in school. Students shall not access entertainment sites, such as social Networking sites (Example: Blogs) or gaming sites, except for legitimate educational purposes under the supervision of an instructor or other professional. District Staff members and students who personally participate in social networking web sites are prohibited from posting data, documents, photographs, or inappropriate information on any web site that might result in a disruption of classroom or District activity. The Superintendent/designee has full discretion in determining when a disruption of classroom or District activity has occurred. District staff is prohibited from providing social networking web site passwords to students. Fraternalization between District Staff and students via the Internet, personal email accounts, social networking web sites, and other modes of virtual technology is also prohibited. Violation of the prohibitions listed above will result in staff and/or student discipline in accordance with State law, Board policies and regulations, the Student Code of Conduct and/or staff negotiated agreements. Nothing in this policy prohibits District staff and students from the use of education web sites.

**10. *Personal Mobile and Portable Devices***

All student use of the District Internet system or personal cell phones, laptops, tablets, digital cameras or other electronic devices is subject to the provisions of the Disciplinary Code. Students may not share or post personal information about or images of any other student or staff member. If a student is found to have used a personal cell phone or digital device in a manner that is not in accord with this Acceptable Use Policy, in addition to other disciplinary actions, the administrator may ban the student's use of any personal electronic device. All computer resources that are considered portable devices are subject to additional security requirements as set out in the District guidelines below. Users shall abide by all requirements established by the District for such portable devices, including but not limited to those related to laptops, tablets, cell phones, smart phones, USB memory sticks, and portable hard drives.

**Personal Mobile and Portable Devices Guidelines**

All student use of personal cell phones, laptops, tablets, digital cameras or other electronic devices is subject to the provisions of the Disciplinary Code and must be used in accordance with the Student Computer Acceptable Use Policy.

Student use of personal cell phones, laptops, tablets, digital cameras or other electronic devices are limited to designated times and areas as outlined in the student handbook or with the permission of the District Staff or Administration for legitimate purposes.

All network access by personal mobile or portable electronic devices is to be through the District's network and is subject to the Student Computer Acceptable Use Policy. Accessing other networks (such as 3G or 4G) are considered a violation of the Student Computer Acceptable Use Policy and the student is subject to disciplinary action as outlined in the Student Computer Acceptable Use Policy.

**11. *New Technologies***

New network technologies are being invented constantly, and it is impossible to predict what systems or applications will be available for use in the future. The requirements of this policy apply to all technologies currently in use on the District Network and those technologies that may be used in the future on the District network. The District shall establish guidelines on the use of any new technology approved for use on the District Network

**12. *Student Expressions on Web Sites & Blogs (Off School Grounds Actions)***

Maintaining or posting material to a web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students and/or staff to participate fully in school or extracurricular activities, is a violation of the student disciplinary code and subject to appropriate discipline.

**13. *Web Sites***

Web sites created through the Network and/or linked with the District's official web site must relate specifically to District-sanctioned activities, programs or events. Web sites created using the Network or the District's equipment, or web sites created as part of a classroom or club assignment or activity are the sole and exclusive property of the District. The District reserves the right to require that all material and/or links with other sites found to be objectionable be altered or removed.

As part of class/course assignments, students may be developing and or/publishing content to the web via web pages, blogs, wikis, podcasts, vodcasts, and webcasts, or may be participating in videoconferences:

1. Personal Information such as phone numbers, addresses, e-mail addresses or other specific personal information shall not be published or shared to a public page or videoconference.
2. All web content must comply with this policy.
3. All web content and videoconferencing must be under the direction and supervision of an instructor or school administrator and is to be used for educational purposes only.
4. All web content is subject to copyright laws and fair use guidelines.
5. All web content shall only be posted to District-approved web pages, blogs, wikis, podcasts, webcasts, vodcasts and videoconferences.

**14. *Workstation Configuration***

The user agrees to not modify the configuration of any workstation. Prohibited changes include but are not limited to: installation of software or downloaded programs, changing desktop wallpaper / background, screensavers, and proxy settings.

**15. *Failure to Follow Policy***

Your use of the Network is a privilege, not a right. If you violate this Policy, you are subject to disciplinary action. At a minimum you will be subject to having your access to the Network terminated, which the District may refuse to reinstate for the remainder of your time as a student at Pike County Joint Vocational School District. At the maximum, you may be suspended or expelled and additional disciplinary action may be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

You breach this Policy not only by violating the above Policy yourself, but also by failing to report any violations by other users that come to your attention. A violation of this Policy may also be a violation of the law and subject the user to criminal or civil investigation and prosecution.

It is a violation of this policy to use any electronic technology, including but not limited to any software, hardware, or externally provided service, or to do any other act in an effort to disguise your Network or Internet activities that would otherwise be a violation of this policy.

**16. *Warranties and Indemnification***

The District makes no warranties of any kind, either express or implied, in connection with its provision of access to or use of its Network. It shall not be responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any student arising out of the student's use of, or inability to use, the Network. Each student is responsible for backing up his or her files. The District is not responsible for the accuracy of information obtained through electronic information resources, and this information should be used at the student's own risk.

By accessing the Network, you are agreeing to cooperate with the District in the event of the District's initiating an investigation of use or access to the Network through your account, whether that use is on a District computer or on another computer outside of the Network. By accessing the Network, you are further agreeing to indemnify and hold the District and the Data Acquisition Site and all of their administrators, instructors and staff harmless from any and all loss, costs, claims or damages (including attorneys' fees) resulting from access to and use of the Network through your account, including but not limited to any fees or charges incurred through purchases of goods or services by the user.

**17. *Updates***

You may be asked from time to time to provide new or additional registration and account information to reflect developments in the law or technology. You must provide this information in order for you to continue receiving access to the Network. If, after you have provided your account information, some or all of the information changes, you must notify the District Technology Coordinator or other person designated by the District to receive this information.

**18. *District Equipment taken off District Property***

The District must execute property accounting procedures designed to ensure the accuracy of records regarding the acquisition, maintenance, control and disposition of equipment and property. Under certain circumstances, the District will permit checkout of equipment for use on or in some cases off the property for completion of academic, teaching, or administrative assignments. Individuals borrowing District equipment assume full responsibility for the care and security of such property. A combination of accurate accounting records and strong internal controls must be in place in order to detect and protect against loss and unauthorized use of District property. Individuals borrowing property of the District from the Technology Department or Media Center are required to complete the appropriate documentation, so that equipment inventories will accurately reflect the disposition of all the property of the District.

**RESPONSIBILITIES:**

Equipment loaned out for use during or outside of the school day with the authorization of the appropriate Department Head is the responsibility of that student who borrows the item. Loss or damage due to negligence (such as leaving a laptop, camera or any other equipment lying around unattended) may result in a charge to that individual of the replacement cost of the item. Any student checking out equipment (for either "onsite" or overnight use) will be personally responsible and liable for its safeguard and return in serviceable condition. Individuals who cause damage or loss, or who have an item stolen, will be charged the full purchase cost of replacement equipment. For equipment checked out to **students for overnight use**, the form that must be signed by the parent/guardian specifies that they are assuming financial responsibility for the item-- and can be held liable for *any* loss or damage to the item (normal wear out or

equipment breakdown not included). **In all cases**, the equipment is to be returned upon completion of the designated project, or any time at the discretion of the Technology Coordinator and/or Library Media Specialist, or any District administrator for any reason.

## **Internet Safety**

### **General Warning; Responsibility of Parents and Users**

All users and their parents/guardians are advised that access to the Network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her own use of the computer Network, Internet and E-mail systems, and should stay away from inappropriate material and/or sites. Parents of minors are the best guide to help them understand which materials should be shunned. If a student finds that other users are visiting harmful or offensive sites, or if he or she is able to access inappropriate sites, he or she should report such use to the person designated by the school immediately.

### **Personal Safety**

Be Safe. In using the computer Network, Internet and email, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining permission from a supervising instructor or District administrator. Do not arrange face to face meetings with someone you meet on the Internet or through E-mail without your parents'/guardians' permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet or through E-mail in a secluded place or private setting.

### **Protecting Children in the 21st Century Act of 2008**

On August 21, 2011, the Federal Communication Commission released an amendment to the Children Internet Protection Act which includes an E-Rate provision of the Protecting Children in the 21st Century Act of 2008. The FCC order (FCC 11-125) implements the “educating” requirements of the Protecting Children Act effective FY 2012, meaning any school or school district applying for E-Rate discounts **MUST** provide Internet Safety Policies that include “monitoring the online activities of minors and must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and cyber bullying awareness and response.”

We will continue to monitor and filter our internet content with our local filtering appliance, and pass our local filtering through our regional Data Acquisition Site.

The Pike County Joint Vocational School District has adopted a curriculum to address internet safety and bullying. The Pike County Joint Vocational School will use the curriculum as well as resources from other sources that will best meet the current and future needs of our students and staff. The curriculum will help our educators empower their students and the school community to be safe, responsible, and savvy as they navigate the digital world. Our curriculum will be based on three major topic strands with varying age appropriate subtopics, lessons, and strategies. These topics are:

- A. Safety and Security
- B. Digital Citizenship
- C. Research and Information Literacy

### **“Hacking” and Other Illegal Activities**

It is a violation of this policy to use the School's computer Network or the Internet to gain unauthorized access to other computer systems or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic material, or which violates any other applicable law or municipal code, is strictly prohibited. Any attempt to bypass District Internet filtering is strictly prohibited.

### **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 or, if the student is 18 or over, the permission of the student. Users should not give out private information about themselves or others. A supervising instructor or District administrator may authorize the release of directory information as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.

### **Active Restriction Measures**

The school, either by itself or in combination with other schools and the Data Acquisition Site providing Internet services, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) Obscene, (2) Child Pornography, (3) Harmful to minors. The school will also monitor the online activities of students through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors. Internet filtering software or other technology-based protection systems may be disabled by a Technology Coordinator or District administrator, as necessary, for the purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term "harmful to minors" as used herein shall have the same meaning as defined in the Communications Act of 1934 (47 USC Section 254 [h][7]).

### **Penalties for Improper Use**

The use of the District network is a privilege, not a right, and misuse will result in the restriction or cancellation of the use. The principal, instructor, site administrator, supervisor, or systems administrator may limit, suspend, or revoke access to the network at any time. Misuse may also lead to disciplinary and/or legal action for students, including suspension, expulsion, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

### **Disclaimer**

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations that result or have alleged to have resulted from the use of or inability to use the network; or that results from mistakes, omissions, interruptions, deletion of files, loss of data, errors, defects, delays in operations, or transmission or any failure of performance, communications failure, theft, destruction or unauthorized access to the District's records, programs, or services. The District further denies any responsibility for the accuracy or quality of information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

### **Addendum:**

Consent Form Regarding Release of Student Information

