

Paint Valley Local School District

Computer Network and Internet Acceptable Use Policy for Staff

The Paint Valley Local School District (the school district) is pleased to make available to each staff member access to interconnected computer systems, computer equipment, computer programs, the Internet, electronic mail and other new technologies within the school district (collectively, the Network).

Access to the school district's Network is provided as a privilege and as an employment tool only. In order to continue enjoying access to the Network, each staff member must take responsibility for appropriate and lawful use of this privilege. Staff members are responsible for professional behavior on the Network just as they are in a classroom, school hallway or other school district property. While the school district may make reasonable efforts to supervise staff member use of Network access, the ultimate responsibility for exercising and promoting responsible use of this access is that of the staff member.

This document shall constitute the school district's computer Network and Internet Acceptable Use Policy for staff members and applies to all employees who use or otherwise access the Network either on-site or remotely. A copy of this policy shall be provided to staff members.

Each staff member is responsible for reading and abiding by this policy and the Acceptable Use Policy for students. If you have any questions about the provisions of these policies, you should contact the administrator in your school building or the district's technology supervisor. Any use of your account that violates these policies may result in your access being withdrawn and/or additional disciplinary action.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 terms of employment and may result in disciplinary action up to and including termination in accordance with state law and collective bargaining agreements and referral to law enforcement. The district reserves the right to seek reimbursement of expenses or damages arising from 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 the district's technology supervisor. Misuse means any violation of this policy, such as commercial use of these resources, criminal activity, inappropriate content of e-mail, 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. Staff members shall not share their passwords or otherwise allow

anyone to gain unauthorized access to the Network or the Internet. A staff member is subject to disciplinary action for any violations of this policy committed by someone else who, with the staff member's express or implied permission or through the staff member's negligence, accesses the Network with the staff member's password.

4. *Purpose and Use*

The school district is providing you access to its Network primarily to support legitimate district business. Other brief, incidental and personal uses are permitted from time to time (e.g., receiving an e-mail from a spouse regarding a change in dinner plans, or from a son or daughter about the starting time of a track meet.) 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 the building administrator or the district's technology supervisor to help you decide if a use is appropriate.

5. *Equipment, Desktop and Laptop, etc.*

The Paint Valley Local School District (ALSD) provides technology for teachers and students to enhance the teaching process. This equipment in the classroom, or individually approved laptops and equipment that at times may be taken home, are the property of Paint Valley Local Schools and need to be regarded with care. Any misuse or failure of equipment needs to be reported to the technology supervisor. Periodic maintenance on laptops or other hardware is required to ensure a safe and reliable tool for the staff. It is your responsibility to make such equipment timely available for maintenance at the request of the technology supervisor. Failure to abide by the above is considered a violation of this policy and failure to provide the equipment when requested may result in disciplinary procedures up to and including termination in accordance with state law and collective bargaining agreements and referral to law enforcement as well as being financially responsible for expenses for any equipment repair arising from violation of this policy.

6. *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 school 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) Using the Network in a manner inconsistent with the professional expectations of a district employee. When using the Network, users should remember that they are representing the district each time the account is used. Communications on the Network need not be formal, but must be professional in appearance and tone.

7. *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) Engaging in harassment, stalking, or other repetitive unwanted communication, or using the Internet in support of such activities
 - (vii) 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 a virus, worm, Trojan horse, 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”). Accessing the Internet for information to be used in a private business, or the transmission of e-mails or other communications between yourself and private business associates or clients of a private business are likewise prohibited

- (d) **Uses or activities that are unrelated to legitimate District purposes**, other than brief, incidental, personal uses that are permitted subject to proper use. Users may not, during the work day, access the Internet for purposes of personal shopping, buying or selling items of real or personal property, researching or making arrangements for non-work-related travel, connecting with a personal web site or weblog, receiving or posting messages to non-work-related web sites or weblogs, participating in any type of gaming activity, engaging in social or hobby activities, for purposes of engaging in or supporting any kind of business or other profit-making activity, or for general recreational web browsing. (*Examples:* Amazon, eBay, Expedia, Grudge Report, dating services, chat rooms, poker web sites, CNN, ESPN.)
- (e) **Using non-district e-mail.** All use of e-mail must be through the school district’s e-mail service. The use of other providers of e-mail (such as Hotmail or Yahoo) through the Network is prohibited. Use of e-mail for non-district purposes, such as for operation of private business enterprises, is strictly prohibited. Only brief, incidental and completely personal uses which are not commercial, political, or whose content does not otherwise violate this policy are permitted from time to time.
- (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 a school district administrator and technology supervisor. Staff members may not move, repair, reconfigure, modify or attach any external devices to Network equipment, computers or systems. Staff members shall not remove, alter or copy district software for their own personal use or for the use of others.

8. ***Confidentiality***

The confidentiality of any information stored in, or created, received or sent over the e-mail system or through Internet access cannot be assured. To the extent feasible, staff members should therefore avoid transmitting confidential information over the e-mail system or through Internet access. If personal information about an individual student must be transmitted, an effort should be made to

make the information not “personally identifiable”, e.g. by not connecting the student’s full name to the information. All e-mails created by a staff member containing confidential information must have a “Private and Confidential” disclaimer appended to the e-mail.

9. Privacy

Network access is provided as a tool for District business. The school 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 school district and you should not have any expectation of privacy regarding those materials. Network 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.

10. Laptop Usage

District employees may be issued a laptop computer to be used inside and outside of school in order to enhance, enrich and facilitate teaching and administrative duties. These laptop computers are subject to the same acceptable use guidelines provided by this policy. In addition, employees issued a laptop computer accept further responsibility regarding the safekeeping of these computers. Employees will be held personally liable for damage to or theft of District laptop computers as a result of the employee’s negligence. Employee’s to be issued a District laptop computer must acknowledge their responsibilities by agreeing to and signing the District’s Laptop Use and Security Agreement.

11. Web Sites

Web sites created through the Network and/or linked with the school district’s official web site must relate specifically to district-sanctioned activities, programs or events. Web sites created using the Network or the school 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 school district. The school district reserves the right to require that all material and/or links with other sites found to be objectionable be altered or removed. As appropriate, the school district may also request such a disclaimer on external web sites that relate directly to school district activities, programs or events.

12. Failure to Follow Policy

Your use of the Network is a privilege, not a right. If you violate this policy, you may be subject to disciplinary action. At a minimum you will be subject to having your access to the Network terminated, which the school district may refuse to reinstate for the remainder of your employment by the school district. At the maximum, your employment may be terminated for violations. Disciplinary action will be in accordance with applicable state law and collective bargaining agreements.

You breach this policy not only by affirmatively violating the above policy, 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.

13. Warranties and Indemnification

The school 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 staff member arising out of the staff member's use of, or inability to use, the Network. Each staff member is responsible for backing up his or her files. The school district is not responsible for the accuracy of information obtained through electronic information resources, and this information should be used at the staff member's own risk.

By accessing the Network, you are agreeing to cooperate with the school district in the event of the school district's initiating an investigation of use or access to the Network through your account, whether that use is on a school district computer or on another computer outside of the Network. By accessing the Network, you are further agreeing to indemnify and hold the school district and the Data Acquisition Site and all of their administrators, teachers 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.

14. 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's technology supervisor or other person designated by the school district to receive this information.

**ACCEPTABLE USE AND INTERNET POLICY
EMPLOYEE AGREEMENT**

I have read, understood and agree to abide by the Acceptable Use and Internet Safety Policy. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

Printed Name of User

Date

Signature of User

Addendums:

Data Analysis For Student Learning (DASL) User agreement

Consent Form Regarding Release Of Staff Information

District Email Policy.

Laptop Use and Security Agreement

Addendum #1

Paint Valley Local School District

**DATA ANALYSIS FOR STUDENT LEARNING (DASL)
USER AGREEMENT**

As a necessary part of my employment by Paint Valley Local School District, I understand that I am being given access to protected, highly-confidential student information through the Data Analysis for Student Learning (DASL) system, including its Progress Book and other modules.

By signing this agreement, I understand and acknowledge that I am responsible for guarding the privacy of our students and parents by maintaining the confidentiality of this information. I further acknowledge that my breach of this confidentiality is a violation of both Federal and State laws. (20 U.S.C. 1232g, Family Educational Rights and Privacy Act (“FERPA”), Ohio Revised Code 3319.321) I understand and accept that my disclosure of this information to any unauthorized person, whether through negligence or intentional disclosure, may result in both legal liability and in employment discipline up to and including termination.

I hereby agree to use extreme discretion in using and displaying information in the DASL system; I will not leave a computer unattended displaying information or logged into the system; I will not display information where it can be seen by unauthorized users; I will guard my access to this system and not share the password with others; I will maintain the security of any information printed or copied from the system; and I further represent that I have been fully informed as to all policies, procedures and laws that apply to access to student information, and that I understand and will comply with them.

Please Print Name

Date

Signature

Addendum #2

Paint Valley Local School District

Consent Form Regarding Release of Staff Information

Staff Name _____ Position _____

I. Permission to Display Photograph, Audio, Video or Electronic Images

I give my consent (or do not give consent) for photographs, audio, video, or electronic images of myself, to be used by the Paint Valley Local School District for exhibition, public display, publication, publicity materials, advertising, a news media story, video, audio, or other electronic media, such as the Internet, television, CD-ROM, or DVD. I understand that my full name may also be used with such display and may be used on the District's Website.

_____ I give my consent. _____ I do not give my consent.

II. Permission for News Stories

I give consent (or do not give consent) for quoted statements given by me, or photographs, audio, video, or electronic images of myself, with possible identification by full name, to be used for the purpose of news stories or interviews about Paint Valley Local School District or educational experiences by our area news media.

_____ I give my consent. _____ I do not give my consent.

Signature of staff member

Date

Printed name of staff member

Addendum #3

Paint Valley Local School District

District Email Policy

On December 1, 2006, Congress passed legislation stating that schools, businesses, and other organizations are required to keep tabs on all Email, instant messages (IM), and other digital communications produced by their employees. The rules, first approved by the U.S. Supreme Court in April, have been widely reported as important for businesses and other for-profit enterprises. But, according to legal experts familiar with the case, the High Court's ruling also applies to public schools and other nonprofit organizations. SCOCA and the Great Seal Network are working on solutions to archive email. In the meantime, please follow these **guidelines**:

1. Any email communication containing student information must be archived.
2. Any email communication containing information about another employee must be archived.
3. Any email communication pertaining to routine operations, programs, services or projects must be archived.
4. Transitory email communication does not need to be archived. Examples of transitory information are internal meeting notices and routine office communication that does not contain employee or student information.

If you use an email client, such as Outlook or Outlook Express, it is recommended that you place your email in folders. Another archival method is to print out and save a copy of the email communication. If you use the Great Seal Network Mail, the client software saves all incoming and outgoing email. It is recommended that you create folders to organize your email and print and save a copy of the email communications listed above. As a result of legislations, it is highly recommended that you do not use your personal email account for communication with staff, parents and students. If you were involved in litigation, it would be very difficult to obtain the necessary information.

Addendum #4

LAPTOP USE AND SECURITY AGREEMENT

As an Paint Valley Local School District employee, I understand that the laptop computer assigned to me remains the property of the Paint Valley Local School District. I agree to the following:

Laptop Use

- Laptop computer use is subject to the District's Acceptable Use Policy. I agree to the terms of this policy and have acknowledged such by signing a Staff District Acceptable Use Policy.
- Laptop computers must be at school and connected to the District Network each day the District is in session to ensure regular anti-virus and software updates.
- I am permitted to take the laptop computer issued to me off-site at the end of the school day, but am personally responsible for securing it as described below.
- I may not install any hardware or software on the laptop computer issued to me without permission from the District Technology Supervisor.
- I will not connect the laptop computer issued to me to my home Internet connection or any other external network without first consulting the District Technology Supervisor. It is the sole discretion of the Technology Supervisor whether an external network provides an appropriate environment for District's laptop computers.
- I understand that I may not lend the laptop computer issued to me to anyone for any reason, unless it is approved by my direct supervisor and the new user completes this agreement. This provision does not apply to in-classroom use by other students or employees in your presence and under your supervision.
- In the event my employment with the District terminates for any reason, I understand I must immediately turn in my laptop computer to my administrator.

Security

- I understand that it is my responsibility to secure the laptop computer issued to me, whether it is at school or off-site.
- At school, laptop computers must be kept in a locked classroom or office at a minimum. If available, they should be further secured in a locked desk, cabinet or closet.
- If you take your laptop computer off-site, the following apply:
 - Do not leave the laptop computer in an unattended vehicle regardless of where the vehicle is.
 - Do not subject the laptop computer to extreme temperatures.
 - Carry the laptop computer in a case specifically designed for laptop computers.
 - Lock the laptop computer in a secure location when not in use. An unattended vehicle is not considered secure.
- Adherence to these procedures will minimize the risk of theft. If theft were still to occur, you must report it to law enforcement and the Treasurer immediately.

Damage or theft due to your negligence or failure to follow the terms of this agreement will result in personal liability for such damage or theft. This includes any damage, such as a virus, that could spread to other District network equipment as a result of inappropriate laptop computer use.

Employee's Signature

Administrator's Signature

Employee's Name (Printed)

Administrator's Name (Printed)

Date

Date