Vermilion Parish School Board
Acceptable Use Policy for Internet and District Network Resources

Introduction

The Vermilion Parish School Board (District) shall authorize the Superintendent and designated staff to establish appropriate guidelines for using the Vermilion Parish School Network (Network) and Internet resources within the school district to enhance learning, provide innovative educational opportunities and/or perform activities directly related to your employment. Acceptable use of these resources shall be consistent with the philosophy, goals, and objectives of the District. Any user, including students, employees and/or guests, who wish to use the District's computers and network, including internet, email and/or district-approved apps and services must agree to abide by all district regulations.

Terms and Conditions are provided so that Network users are aware of the responsibilities they will assume when using this VPSB resource. Responsibilities include efficient, ethical and legal utilization of the network resources. The student/employee signature on the VPSB policy is legally binding and indicates that he/she has read the *Terms and Conditions* carefully and agrees to abide by them.

Terms and Conditions
1. **Personal Safety and Privacy**
   a. Users will not publish online any personal contact information (e.g. address, phone number) about themselves or any other person.
   b. Users will not agree to meet with someone they have met online. Inappropriate contacts should be reported to supervising personnel immediately.
   c. It is expected that all students will be appropriately supervised and monitored during any online activities to ensure proper use.
2. **Illegal Activities**
   a. Users will not attempt to circumvent the Network or gain unauthorized access to the Network, any computer system or another person's account or files.
   b. Users will not intentionally attempt to disrupt or intentionally disrupt the computer system, the Network or alter/destroy data by spreading computer viruses or by any other means.
   c. Users will not engage in any illegal activity, such as, but not limited to, illegal drug activity, fraud, engaging in criminal gang activity or threatening the safety of a person or persons, etc.
   d. Users will not attempt to impersonate another individual or organization using VPSB Network or other technology resources for any reason (i.e. phishing).
3. **Security**
   a. Users are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use your account. Under no condition should users give their password to another person nor post the password in written form where others can easily see it.

b. Users will immediately notify supervisors if they have identified a possible security problem. Purposely looking for possible security problems may be considered as an illegal attempt to gain access. Any security concerns should be addressed to the VPSB Tech Support Center.

c. Users will log off or lock their accounts when away from the computer for an extended period to prevent unauthorized access.

d. Users will avoid the spread of computer viruses by ensuring that their district computer has up-to-date antivirus software provided by the district. The user may not remove, disable or replace the district antivirus software solution for any reason.

e. Users will not download and install unnecessary programs from the Internet or external devices since most of this installs spyware/malware on the computer and hinders the performance of the computer (i.e. Toolbar helpers, email add-ons, screensavers, search engine assistants, etc.)

f. Users should be aware that the VPSB Network, Internet use and system email (with associated apps) is maintained and regularly monitored for inappropriate use. If the staff detect any misuse, appropriate disciplinary action will be taken against the person or persons involved.

g. Users are not allowed to install software to capture or monitor the computer activity of other users on the network or network traffic. Only authorized VPSB tech support staff is permitted to do this in the course of administering the network.

h. The use of the Internet, email,

i. and district approved apps is a privilege of employment or student registration with the district. Upon leaving the district as an employee or student, all accounts will be inactivated.

4. Network

a. All computers are to be set up and maintained with connection to the VPSB domain for network administration and security. Removing a computer from the VPSB domain without the permission of a VPSB tech support staff member will be considered an act to circumvent district network security and is strictly prohibited.

b. All wireless devices on the VPSB Network will be set up using official VPSB wireless policies. All wireless devices purchased must be equipment approved by the network department. No unauthorized wireless devices will be attached to the VPSB network. Doing so will be considered a network security breach and dealt with accordingly.

c. Network bandwidth is a limited resource that must be conserved to serve all of the network needs of the district. Users must understand that the use of rich Internet content (i.e. listening to streaming audio, viewing streaming video sites and downloading extremely large files, etc.) should not be abused where it affects network use by others.

d. Important information regarding the VPSB network will be sent out to all employees from time to time during the year addressed from the email account "techbytes@vpsb.net". It is the responsibility of all employees to open and read all emails from this account and then act accordingly. Excuses such as "not reading" or deleting the messages from this account will not be acceptable.

5. Inappropriate Content

a. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, unprofessional or disrespectful language in any electronic form using the VPSB Network. This includes personal attacks or harassment of another person.
b. Users will not use the VPSB network to access obscene, profane, lewd, vulgar, rude, inflammatory, threatening, unprofessional or disrespectful content in any electronic form including audio, images, video and text.
c. Users will not circumvent district content filters using any means in order to access inappropriate content as listed above.
d. Users will immediately report to their supervisors any website they access that has inappropriate content.

6.   Resource Limits
a. Users will use the system email, Internet and network resources only for educational, professional development and work-related activities. Using work resources for personal purposes is unacceptable as well as using personal email for work-related purposes. This included using district network resources for email, personal monetary gain (such as operating a personal business) or shopping online for personal needs.
b. Users will not post or forward email chain letters, jokes or send annoying or unnecessary messages to others.
c. Users will not use district email to mass email users (internal and external) with unauthorized communications or solicitations.
d. Users will subscribe only to high-quality discussion groups and information feeds that are relevant to educational or professional activities. Users will not subscribe others to such services without their consent.

7.   Access and Use of Materials
a. Users will not plagiarize, defined as taking the ideas or writings of others and presenting them as if they were their own. This includes but is not limited to items on the internet, discussions groups, books, etc.
b. Users will respect copyrighted materials and other intellectual property. Users may not duplicate, copy or distribute electronic resources without the appropriate permissions, documentation or citations.

User Rights
1. Free Speech
a. The right to free speech applies also to communications on the Internet. The Network is considered a limited forum, similar to the school newspaper, and therefore the District may restrict a user's speech for valid educational purposes.

2. Search and Seizure
a. Users should expect only limited privacy in the contents of personal files on the District system.
b. Routine maintenance and monitoring of the Network may lead to a discovery that a user has violated District policy, or regulations, or the law.
c. An individual search will be conducted if there is reasonable suspicion that a user has violated District policy, or regulations, or the law. The investigation will be reasonable and related to the suspected violation.

3. Due Process
   a. The District will cooperate fully with local, state, or federal officials in any investigation related to any misuse of District computers or the Network.
   b. In the event there is a claim that someone has violated District policy or regulations in the use of the Network, the user will be provided with written notice of the suspected violation and an opportunity to present an explanation before a neutral administrator.

Consequences of Misuse
1. The use of the Network services, Email and Internet is a privilege, not a right, and inappropriate use will result in a cancellation of privileges and/or other disciplinary action (including disabling account(s) and permission(s), suspension, termination or legal action) as deemed appropriate by administration, faculty, and staff.
2. Users should expect no privacy of the contents of personal files and information on district computers and email on the district system. Messages relating to, or in the support of Illegal activities must and will be reported to the authorities.
3. Misuse of the system can result in possible legal action and/or prosecution and will require restitution for costs associated with the system restoration, hardware or software costs.
4. Users bringing illegal and/or inappropriate materials into the system's electronic environment will be subject to disciplinary action.

Disclaimer

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor-supplied hardware and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system, will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, not that defects will be corrected. Opinions, advice, services and all other information expressed by system users, information providers, service providers or other third party individuals in the system are those of the providers and not necessarily the District. The District will cooperate fully with local, state or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks.

Adopted 5/8/19