Policy 2361 ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

The Board of Education recognizes as new technologies shift the manner in which information is accessed, communicated, and transferred; these changes will alter the nature of teaching and learning. Access to technology will allow pupils to explore databases, libraries, Internet sites, and bulletin boards while exchanging information with individuals throughout the world. The Board supports access by pupils to these information sources but reserves the right to limit in-school use to materials appropriate for educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes technology allows pupils access to information sources that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer networks and declares unethical, unacceptable, or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The Board provides access to computer networks/computers for educational purposes only. The Board retains the right to restrict or terminate pupil access to computer networks/computers at any time, for any reason. School district personnel will monitor networks and online activity to maintain the integrity of the networks, ensure their proper use, and ensure compliance with Federal and State laws that regulate Internet safety.

Standards for Use of Computer Networks

Any individual engaging in the following actions when using computer networks/computers shall be subject to discipline or legal action:

A. Using the computer networks/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate Federal, State, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the networks. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.

B. Using the computer networks/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.

C. Using the computer networks in a manner that:
   1. Intentionally disrupts network traffic or crashes the network;
   2. Degrades or disrupts equipment or system performance;
   3. Uses the computing resources of the school district for commercial purposes, financial gain, or fraud;
   4. Steals data or other intellectual property;

5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another person;
6. Gains or seeks unauthorized access to resources or entities;
7. Forges electronic mail messages or uses an account owned by others;
8. Invades privacy of others;
9. Posts anonymous messages;
10. Possesses any data which is a violation of this Policy; and/or
11. Engages in other activities that do not advance the educational purposes for which computer networks/computers are provided.

Internet Safety Protection

As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. The technology protection must block and/or filter material and visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other material or visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and world wide web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the material and visual depictions prohibited in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent of Schools or designee will develop and ensure education is provided to every pupil regarding appropriate online behavior, including pupils interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361. Any changes in

Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

The school district will certify on an annual basis, that the schools, including media centers/libraries in the district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

Consent Requirement

No pupil shall be allowed to use the school districts' computer networks/computers and the Internet unless they have filed with the Instructional Technology (individual or office) a consent form signed by the pupil and his/her parent(s) or legal guardian(s). **Documentation will be kept in the student database and will apply for the duration of the pupil's schooling in the Vineland School District unless changed in writing and signed by the pupil and his/her parent(s) or legal guardians.**

Violations

Individuals violating this Policy shall be subject to the consequences as indicated in Regulation 2361 and other appropriate discipline, which includes but are not limited to:

1. Use of the network only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act.
Federal Communications Commission: Neighborhood Children's Internet Protection Act

Adopted: 09 June 2010
REVISED: 13 June 2012
REVISED: 13 May 2015

2361.1 INTERNET USE

Internet access is now available to pupils and teachers in the Vineland Public Schools. The Board of Education is pleased to bring this access to Vineland Public Schools and believes the Internet offers vast, diverse, and unique resources to both pupils and teachers. The Board's goal in providing this service to teachers and pupils is to promote educational excellence in schools by facilitating resource sharing, innovation, and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Pupils and teachers have access to:

1 Electronic mail communication with people all over the world.

2. Information and news from NASA as well as the opportunity to correspond with the scientists at NASA and other research institutions.

3. Public domain software and shareware of all types.

4. Discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics.

5. Access to many University Library Catalogs, the Library of Congress and ERIC.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Vineland Public Schools has taken precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. The Board firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the Vineland Public Schools.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. This policy is provided so that all are aware of the responsibilities each is about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a Vineland Public Schools user violates any of these provisions, future access could possibly be denied.

Internet Terms and Conditions

1. Acceptable Use - The purpose of NSFNET, which is the backbone network to the Internet, is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work.

   The use of Internet must be in support of education and research and consistent with the educational objectives of the Vineland Public Schools. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

2. Privileges - The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. Each pupil who has access to the Internet will be part of a discussion with a Vineland Public Schools faculty member pertaining to the proper use of the network. The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as required. The administration, faculty, and staff of Vineland Public Schools may request the system administrator to deny, revoke or suspend specific user accounts. No pupil account may be transferred by a pupil to another pupil nor used by another pupil.

3. Network Etiquette - Pupils are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

   a. Be polite. Do not get abusive in your messages to others.

   b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.

   c. Do not reveal your personal address or phone numbers or any other personal information of pupils or colleagues.

   d. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

   e. Do not use the network in such a way that you would disrupt the use of the network by other users.

f. Do not play games or use the computer resources for other non-academic activities when others require the system for academic purposes.

g. Do not waste nor take supplies, such as paper, printer ribbons, and diskettes, that are provided by Vineland Public Schools in a computer lab.

h. All use of the Internet must be in support of education and research and consistent with the purposes of Vineland Public Schools.

i. Any use of the network for commercial or for-profit purposes is prohibited.

j. Use of the network for personal and private business is prohibited.

k. Any use of the network for product advertisement or political lobbying is prohibited.

l. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.

m. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.

n. All communications and information accessible via the network should be assumed to be private property.

o. No use of the network shall serve to disrupt the use of the network by others; hardware or software shall not be destroyed, modified, or abused in any way.

p. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

q. Hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited on the network.

r. The illegal installation of copyrighted software for use on district computers is prohibited.

s. Use of the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the local area network is prohibited.

t. Any pupil use of Internet "live chat" capabilities will be directly supervised by an administrator, faculty or staff member.

u. Use of network systems (data, video, voice) for soliciting or distributing information with the intent to harass, intimidate, or bully which can be described as Cyber Bullying.

4. Vineland Public Schools makes no warranties of any kind, whether expressed of implied, for the service it is providing. Vineland Public Schools will not be responsible for any damages you suffer. This includes loss of data resulting from delays, nondeliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at user's own risk. Vineland Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through its services.

5. Security - Security on any computer system is a high priority, especially when the system involves many users. If a user feels they can identify a security problem on the Internet, the user must notify a teacher or other staff member or your System Coordinator. Do not demonstrate the problem to other users. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to Internet.

6. Cyber Bullying- As per 2002 New Jersey Law, AB 1874, "the state legislature finds and declares that: a safe and civil environment in school is necessary for pupils to learn and achieve high academic standards; harassment, intimidation or bullying, like other disruptive or violent behaviors, is conduct that disrupts both a pupil's ability to learn and a school's ability to educate its pupils in a safe environment". In compliance with that law, usage and employment of network systems (data, video, or voice) to harass, intimidate, or bully which can be described as Cyber Bullying, is unacceptable. If a pupil feels they are the subject of Cyber Bullying, the pupil should notify a teacher or other school staff member immediately.

7. Vandalism - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or any of the above listed agencies or other networks that are connected to the NSFNET Internet backbone. This includes, but not limited to, the uploading or creation of computer viruses.

8. The user should recognize that software is protected by copyrights laws; therefore, user will not make unauthorized copies of software found on school computers, either by copying them onto his/her own diskettes or onto other computers through electronic mail or bulletin boards; user will not give, lend, or sell copies of software to others unless user has the written permission of the copyright owner or the original software is clearly identified as shareware or in the public domain.

9. The user should recognize also that the work of all users is valuable; therefore, user will protect the privacy of each other's areas by not trying to learn their passwords; user will not copy, change, read, or use files in another user's area, without that user's prior permission; user will not attempt to gain unauthorized access to system programs or computer equipment; user will not use computer systems to disturb or harass other computer users by sending unwanted mail or by other means; and user will not download information onto the hard drives of any Vineland Public School computer for permanent storage.

10. Any user who does not comply with this policy will lose network privileges as determined by the Building Principal. Repeated or severe infractions of this policy may result in termination of access privileges permanently. Pupil infractions may result in appropriate disciplinary action in addition to suspension or termination of access privileges. Unauthorized use of the network, intentional deletion or damage to files and date belonging to other users, or copyright violations may be termed theft as defined under New Jersey Revised Statutes.

11. All Building Principals shall obtain parent's and pupil's consent to these guidelines in the form of a written agreement.

Adopted: 11 June 1997
Revised: 12 October 2005, 09 June 2010

2361.2 ELECTRONIC COMMUNICATION

Background

E-mail and attachments voice mail, video conferencing, access to the Internet, and associated file access are made available to staff members of the Vineland Board of Education (hereinafter, the "V.B.E.") for the purpose of conducting work-related business. Employees provided with these tools are expected to use them in a responsible and productive manner. Employees are also required to acknowledge that all messages and files created, stored, sent or received will remain the property of the V.B.E.. At no time and under no circumstances can personal software be introduced to the V.B.E. computer system. Against this background, the following guidelines have been established to assist employees in the use of these tools.

E-mail ,Voice Mail, Files Data/Video/Voice Systems

The content of e-mail, voice mail messages or any file(s) may not contain anything that would reasonably be considered offensive or disruptive to any employee. Offensive content would include, but is not limited to, sexually explicit material or racial slurs, or any comments that would offend someone on the basis of their age, sex, race, sexual orientation, sexually explicit material, religious or political beliefs, national origin, or disability.

The V.B.E. reserves the right to access and monitor any message or file on the data/video/voice computer(s) system as deemed necessary and appropriate. Messages are public communications and are not private. All communications including text and images may be subject to disclosure to law enforcement or other third parties without prior consent of the sender or the receiver. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and review said message.

Notwithstanding the V.B.E.'s right to retrieve and read any electronic voice or e-mail message, or any files such message or files should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve messages that are not sent to them except when granted electronic proxy rights.

The V.B.E. reserves and will exercise the right to access, review and audit, e-mail system voice logs or messages and/or internet service at any time, with or without employee notice, and that such access may occur during or after working hours.

No audit of e-mail, voice logs or messages or computer records can be conducted without a written request from an Assistant Superintendent, Director or Principal, Supervisor of Technology of the V.B.E., which shall be accompanied by an approval from the Superintendent.

All e-mail and user files will be purged periodically. Network hardware/software monitoring, scanning, or "sniffing" for malicious code or intrusion is restricted to central office network management staff.

No information of any kind, nature or description concerning any matters affecting or relating to the business of the V.B.E., including without limiting the generality of the foregoing, the names or addresses of any of its pupils or employees or academic records or information, compensation programs, contracts, policy terms, or any other information of, about, or concerning the business of the V.B.E., shall be released via the V.B.E. e-mail system unless such information is already officially released or prior written approval is obtained from the Superintendent.

The Internet

Employees granted access to Internet are representing the V.B.E.. Employees are responsible for seeing that the Internet is used in an effective, ethical and lawful manner. The V.B.E. Internet connection should not be used for personal gain or advancement of individual views. Use of the Internet must not be disruptive to the workplace or interfere with productivity.

Each employee is responsible for the content of all text, audio or images that they place or send over the Internet via the V.B.E. connection. Fraudulent, harassing or obscene messages are prohibited. No messages should be transmitted under an assumed name. Users should not attempt to obscure the origin of any message. Information published on the Internet should not violate or infringe upon the rights of others.

No information of any kind, nature or description concerning any matter affecting or relating to the business of the V.B.E., including, without limiting the generality of the foregoing, the names or addresses of any of its students or employees, or academic records or information, compensation programs, contracts, policy terms, or any other information of, about, or concerning the business of the V.B.E. shall be released via the V.B.E. Intranet or the Internet unless such information is already officially released or prior written approval is obtained from a senior officer of the V.B.E.

The V.B.E. will cooperate with proper requests made under the "Freedom of Information Act" and/or regulations promulgated by the State of New Jersey Department of Education, or by any other regulatory body having jurisdiction over the operation of the V.B.E. All such requests must be approved by the Board Secretary after consultation with the Superintendent or Solicitor.

Violations

Violations of a guidelines listed above may result in disciplinary action up to and including termination. If necessary the V.B.E. will advise appropriate legal officials of any illegal violations.

Adopted: 12 December 2001
Revised: 09 June 2010