Policy Title: Electronic Information Resources

Policy Reference: PL.156

Attaches To: (see page 1 and 2, Objects(s): Job Descriptions, Etc, Applied To)

Description:

As outlined in the Utah State Code 53A-3-422, Vanguard shall adopt and enforce a school wide Electronic Information Resource Policy. This policy will apply to both students and employees. Vanguard shall provide to its students and employees the opportunity to utilize electronic information resources. In order to enhance learning, teach computer skills, and effectively utilize modern electronic information resources within the school, students and teachers shall have access to computers and the Internet. Other electronic information resources may include, but are not limited to, voice mail, email, and various network files or accounts.

In an effort to protect students and employees, the school will provide appropriate Internet filtering and monitoring for safety. It must be understood that although Vanguard will make its best efforts to filter content, no system is 100% foolproof. Additionally, both students and employees will be issued usernames and passwords. All use of electronic information within the school must be consistent with the educational objectives of the school; electronic resources within the school are not intended for private, personal, or political use. The Director and/or Technology Specialist may determine appropriateness of use of electronic information resources at his/her discretion.

No individual shall be allowed to use computers and/or the Internet without documentation indicating that the Student Computer/Internet Use Agreement has been carefully read, understood, and that the users agree to abide by the terms and conditions regarding proper behavior and use of all electronic information resources, including computers and the Internet. Student use of electronic resources may be permitted provided the school receives annual documented parental permission and agreement to terms and conditions on behalf of their student. Agreement to terms and conditions is legally binding. All user accounts are subject to Vanguard control and may be revoked for misuse. Violation of any part of this policy will result in disciplinary action according to defined school discipline policy, including the possibility of loss of privilege to use computers and other electronic information resources, suspension, expulsion, loss of employment, and appropriate legal action.

Neither students nor employees shall have any expectation of privacy in regard to utilization of electronic information resources provided by the school. This includes, but is not limited to files, disks, documents, emails, voice mails, etc. which have been created with, entered and stored in, downloaded to, or accessed by Vanguard electronic information resources. Vanguard administration or Board of Directors may monitor, log, and/or review any or all student or employee files and messages.

Acceptable Use of Electronic Information Resources:

All Vanguard Academy employees should:

• Abide by generally accepted rules of network etiquette. These rules include, but are not limited to being polite, kind, and using appropriate language.

• Monitor student’s use of electronic devices. Students should only use computers and other electronic devices with the permission and supervision of teachers of staff and should respect and follow teacher/staff instructions.

• Immediately report accidental access of unauthorized or unacceptable Internet sites to staff/teacher/administration as appropriate.
• Ask for help when unable to properly use computers equipment or other electronic information resource.

Unacceptable Use of Electronic Information Resources: Students and employees must not intentionally:
• Harm or destroy computer equipment through abusive behavior.
• Use school technology and equipment for personal or private use, unrelated to school assignments or responsibilities.
• Allow students to reveal personal information, such as names, addresses, telephone numbers, passwords, credit card numbers, photographs, or social security numbers. Employees are advised against such. All individuals are prohibited against revealing the personal information of others or regarding the school.
• Communicate with language, graphics, or artwork that is considered to be vulgar, defamatory, threatening, or otherwise inappropriate.
• Access, receive, or transmit material that is pornographic, obscene, sexually suggestive or explicit or other material related to weapons, controlled substances or alcohol, or incendiary devices.
• Post or transmit content that that is considered “cyberbullying” as previously defined.
• Post or send content that contains threats or is hatefully or racially, ethically or otherwise objectionable.
• Utilize any electronic devices in school locker rooms, showers or bathrooms.
• Intentionally harm or destroy school data, the network, or general network performance. This includes, but is not limited to:
o Participating in or promoting any illegal or inappropriate activities that change the use of the computer hardware or software.
o Corrupting, destroying, or manipulating system data.
o Hacking or other activity, such as creating, loading, or transmitting viruses or worms, malware, password grabbers, spyware, etc. or other software which may compromise the network
o Erase, expire, or reset memory cache, web page links, or HTTP location history.
• Use one’s identity or misrepresent one’s identity or the identity of another to gain unauthorized access to restricted information, systems, or programs; use the school network to illegally access other systems; or to chat, email, or otherwise communicate electronically.
• Download, upload, install, or execute unapproved software without prior approval for Technology Specialist and/or Administration as appropriate.
• Formally publish school related information on the Internet without proper approvals from administration or Board of Directors. This does not include teacher and/or staff websites that are created to communicate information on assignments and class schedules.
• Violate copyright laws.
• Copy system or curricular programs or files without proper approval.
• Participate in unapproved and non-educational gaming.
• Participate in unapproved interactive real time Internet activity, such as chat rooms.
• Use the network for product advertisement or other business purposes.
• Use the network for political purposes.
• Participate in any activity that is illegal or does not conform to the rules, regulations, and policies of Vanguard.

Neither employees nor students may bring personal electronic equipment such as palm computers or laptops into the school unless they have been approved. All personal devices are subject to the same

policies and guidelines as all school-owned devices.
Vanguard does not make any warranties for the electronic information resources that are provided by the school. Any damages that may be suffered as a result of a student or employee using these resources are not the responsibility of the school. Damages may include, but are not limited to the loss of data as a result of delay, human error or omission, or non-delivery or service interruption caused by a network system. The school cannot be held responsible for the accuracy of information obtained through any of the electronic information resources which it provides. All employees and students use the network system and the information obtained therein at their own risk.
Approved: 08/15/2015

Purpose:

Scope:

Policy Type: ☐Company ☐Position ☐Other _____

Job Description(s) Applied To:

Reference	Job Description (JD) Title(s)
JD: 221	Company Wide

Template Object(s) Applied To:

Reference	Template (TP) Title(s)

Revision History:

Revision #	Date of change	Description of change	Authorized by
1.1	N/A	Launched Object	N/A