



Valley Regional Adult Education (VRAE) Acceptable Technology Use Policy

Technology Use and Monitoring

General Rights, Responsibilities and Duties

VRAE provides computers, computer systems, software, and other electronic resources as well as network access privileges for students and staff to carry out their educational needs.

The computers, computer systems, software, and other electronic resources as well as the network are the property of VRAE and are to be used only for those activities directly related to teaching, learning and/or management by students and staff. The equipment, infrastructure, software and other electronic resources as well as the network are not to be used for personal gain or illicit/illegal activity by any student or staff member.

All users are hereby made aware that all information on VRAE's computers, computer systems, and networks are in the public domain, unless specifically protected by the Connecticut Freedom of Information Act. Therefore, VRAE reserves the right to bypass any or all individual or group passwords to determine the activity on any or all computers, computer systems, software and other electronic resources as well as network access privileges.

VRAE issued email is to be used solely for those activities directly related to the Valley Regional Adult Education.

VRAE retains control, custody and supervision of all computers, networks and Internet services owned or leased by VRAE. VRAE reserves the right to monitor all computer and Internet activity by employees and other system users. Employees and students have no expectation of privacy in their use of school computers, including e-mail messages and stored files.

Employees and students are expected to use appropriate judgment and caution in communication concerning students and staff to ensure that personally identifiable information remains confidential.

Network

The network includes wired and wireless computers and peripheral equipment, files and storage, email, installed software and Internet content. VRAE reserves the right to prioritize the use of, and access to, the network.

All use of the network should support student instruction, research and staff development and be consistent with the mission of VRAE.

Acceptable network use by students and staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participation in Google Apps for Education that support student instruction and staff development;

- The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately.
- Connection of staff and student personal laptops or other computing devices to the VRAE's network after checking with the Technology Coordinator to confirm that the laptop is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all regulations in this document.

Students are expected to adhere to all portions of the Student Acceptable Use Policy. Teachers, staff members, and volunteers who utilize school computers for instructional purposes with students have a duty of care to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the policies and rules concerning student computer and internet use and to enforce them. When, in the course of their duties, employees or volunteers become aware of student violations, they are expected to stop the activity and inform the Director or other appropriate administrator.

Unacceptable network use by students and staff includes but is not limited to:

- Personal gain, unauthorized fundraising, commercial solicitation and compensation of any kind;
- Incurring liability or costs by VRAE;
- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the Director or other appropriate administrator.
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, trojan horses, time bombs and changes to hardware, software and monitoring tools;
- Unauthorized access to other VRAE computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing):
- Accessing, uploading, downloading, storage and/or distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the network. Any such equipment may be confiscated.
- Participating in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, email and web pages that do not support student instruction, research and staff development or promote cyberbullying and harassment of any kind.

VRAE will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the VRAE's computer network or the Internet. VRAE assumes no responsibility for



any unauthorized charges made by employees including but not limited to, credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

Internet Safety

Personal Information and Inappropriate Content:

- Students and staff should not reveal personally identifying information, including, but not limited to, a home address and phone number, email address, usernames and passwords.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class or school website unless the appropriate permission has been verified according to VRAE policy. In accordance with the student handbook definition and requirements students may opt-out of having their information used in this way. If this is done, it will be recorded in the Student Database(LACES) and be considered permanent until revoked.
- If students or staff encounter dangerous or inappropriate information or messages, they must notify the Director.
- Refrain from participating in "chat" rooms or subscribing to Listserv's without permission;
- Be polite in language and demeanor and refrain from publishing libelous statements about any group or individual;
- Refrain from using profanity, obscene or defamatory language, and accessing messages or pictures deemed inappropriate, obscene or pornographic;
- Observe all VRAE rules with regard to proper written and oral communication and appropriate behavior;
- Respect the electronic property of others;
- Prohibited from damaging and/or altering computer hardware and software, computer systems, files, and networks, including the introduction of viruses;
- Observe all VRAE rules and local, state, and federal laws and guidelines (including copyright) while using VRAE resources;
- Prohibited from using the network for commercial purposes, including the purchase or sale of personal goods and services;
- Be aware that network storage areas, like other storage areas (e.g., file cabinets, lockers), and files or communications (e.g., email messages) stored in these areas, may be reviewed by network administrators to ensure system integrity and responsible use.

Filtering and Monitoring



Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA) and other objectionable material. The determination of what constitutes "other objectionable" material is a VRAE decision and will be consistent with the policies of VRAE.

- While filtering software makes it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the Internet filter or conceal Internet activity are prohibited: VPNs, proxies, special ports, modifications to school browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- Email inconsistent with the educational and research mission of VRAE will be considered SPAM and blocked from entering email boxes. On the occasion when spam does make it to a student or staff's email box it should be deleted. Users should notify the Technology Coordinator.
- Internet Use will be supervised. The first line of defense in controlling access to inappropriate material on the Internet is deliberate and consistent monitoring of student access to school computers;
- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a concerted effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of VRAE; and
- Staff must make a concerted effort to monitor, instruct and assist students in the appropriate use of technology.

Copyright

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (title 17, USC) and content is cited appropriately.

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

- Change passwords according to VRAE schedule;
- Do not use another user's account;
- Do not insert passwords into email or other communications;



- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Log off if leaving the computer. Lock the screen may be used for those people who exclusively use 1 computer.

Student Data is Confidential

Staff, as well as students related to their peers, must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

Monitoring/No Expectation of Privacy

VRAE provides the network system, email, and Internet access as a tool for education, research, and staff development in support of VRAE's mission. VRAE reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- email;
- Internet access; and
- Any and all information transmitted or received in connection with network and email use.

No student or staff user should have any expectation of privacy when using the VRAE's network. VRAE reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of Connecticut.

VRAE gives notice to all of its employees and to anyone else who enters its facilities or work locations of the potential use of electronic monitoring in the workplace. "Electronic monitoring" means the collection of information on the VRAE's premises and at any of the VRAE's work locations about the activities or communications of employees and others by any means other than direct, personal observation. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, video-camera, tape or digital recording device or any other type of electromagnetic, photo-electronic or photo-optical system.

VRAE reserves the right in its sole discretion to engage in electronic monitoring on its premises and at any of its work locations at any time for any lawful business purpose, including without limitation, to: (a) access business information; (b) provide a safe and secure work environment; (c) assist in the evaluation of employee work performance; (d) supervise employees to be sure that they are acting consistently with business objectives; (e) investigate suspected misconduct;

(f) assess compliance with VRAE policies and applicable law; and to (g) ensure that the VRAE's operations continue appropriately. The practice will not engage in any electronic monitoring that is prohibited by any applicable state or federal law, including without limitation, by monitoring activities in areas provided for employee private, personal use (such as restrooms) and/or by monitoring for the purpose of interfering with/restraining an employee's rights to engage in protected concerted activities.

The following are examples of the specific types of electronic monitoring that the VRAE may use on its premises and at its work locations:

- * Monitoring of email/other components of the VRAE's computer system
- * Video surveillance
- * Telephone and voicemail monitoring
- * Monitoring using GPS tracking devices

An individual consents to being electronically monitored by VRAE for any lawful business purpose by being employed by VRAE and/or by being on the VRAE's premises or at its work locations.

Website, Blog, Wiki or Other Online Resource Guidelines (see the Social Media Policy 4118.5)

- Web pages, blogs, wikis or other online resources must comply with VRAE rules, local, state, and federal laws and regulations.
- Content of web pages, blogs, wikis or other online resources should be consistent with the mission statement of VRAE and support the work of the VRAE. Staff who use the network to post instructional websites, blogs, wikis or other online resources should follow school guidelines for size, scope, and content.
- No individual may post profane, libelous, or defamatory statements about any group or individual.
- Staff members must inform the Director of posted web sites.
- Students may only post web sites under the guidance and supervision of a teacher and should conform to school guidelines for size, scope, and content. Student web sites must be related to the curriculum and must be reviewed by the classroom teacher with prior permission of the Director.
- Personal information about staff and/or students, including personal telephone numbers and addresses, may not be posted on web sites. Individual photographs with student names should not be included without first reviewing the need with Director.
- Any information posted on web sites must be the original material of VRAE staff or students or be in the public domain. All materials will be held to the same publishing standards and criteria as print publications. Copyrighted material, text, or graphics may only be used with the written permission of author or publisher.



- VRAE reserves the right to publish student work on its web site. Such work will be identified only by first name and last initial. Official school newspapers and newsletters are exempt from this guideline.
- While teachers and staff are encouraged to publish their work voluntarily, VRAE will obtain permission from staff members prior to posting their individual work or creations on the school's web site, Internet, or on-line databases. Collaborative work done for the school may be published without permission.
- All curriculum is the property of VRAE and may be published on the school web site and/or network using approved tools.
- Commercial use of web pages for endorsements (i.e., fundraising) will be subject to school policy and review.
- Links to support groups or organizations officially recognized by VRAE will be allowed with the approval of the Director.

Email Communication Guidelines

Students, teachers, and administrators are encouraged to communicate via email, in accordance with the guidelines listed in this policy.

Examples of acceptable use are:

1. Student queries to set an appointment for a conference or request a phone call
2. Student request for recommendations for a tutor, musical instrument teacher, etc.
3. Students responding to teacher request for volunteers
4. General subject matter or curriculum-related questions
5. Questions about a long-term assignment

Examples of unacceptable use are:

1. Communications that harass or threaten any student or employee of VRAE.
2. Frivolous communications (i.e., the latest jokes, etc. forwarded amongst friends).

VRAE expects students to recognize and understand that teacher/administrator schedules vary and that they may not be able to respond to email questions and communications immediately. Teachers will be expected to respond to acceptable email matters (as outlined above) in a timely manner.

- Email use must comply with school rules, local, state, and federal laws and regulations.
- Users should consider all email to be subject to Freedom of Information laws. Therefore, the school reserves the right to bypass any or all passwords to determine email activity.



- Email is to be used for those activities directly related to activities concerning Valley Regional Adult Education.
- The equipment, infrastructure and software are not to be used for personal gain or illicit/illegal activity by any student or staff members.
- Be polite in language and demeanor and refrain from making libelous statements about any group or individual.
- Spamming (sending unsolicited junk mail) and chain letters is prohibited.
- Care should be given with confidential or personal matters to ensure they remain private.
- Password sharing, accounting sharing, thwarting security, anonymous communication, and concealing one's identity are prohibited.
- Users will be liable for any unauthorized costs incurred by the school.
- Users should delete emails in accordance with the Connecticut State Library Retention guidelines or as required by law.
- Users should not open email from unknown sources.

Disciplinary Action

All users of the VRAE's electronic resources are required to comply with the Acceptable Use and Monitoring Policy described above.

Violation of any of the conditions of use will be cause for disciplinary action, including suspension or revocation of network and computer access privileges of employees and students as well as other permissible disciplinary actions as defined in other student and staff policies and administered by VRAE. Any employee who is determined to have engaged in any conduct that is contrary to the VRAE's activities as a result of information obtained through the VRAE's use of electronic monitoring shall be subject to disciplinary action, up to and including termination of employment.

The employee or student shall be responsible for any losses, costs or damages incurred by the school related to violations of school policy or these regulations for which they are responsible.

In addition, criminal penalties and fines may apply where the conduct of the employee or student violates applicable state or federal laws.

Employee Acknowledgement

Each employee and student authorized to access the schools' computers, networks, and Internet services is required to acknowledge that they have read and understood this policy and regulations.

June 1, 2023