VIRTUAL LEARNING ACADEMY CHARTER SCHOOL POLICY

EMPLOYEE ACCEPTABLE USE POLICY GBEA

Goals:

The goal of Virtual Learning Academy (VLACS) in providing the technology resources, network services, the Internet and related technology, is to enhance the education provided to students by:

- Using new and emerging distance learning technologies to provide anytime and anywhere access to a rigorous personalized education that helps students learn today, graduate tomorrow and prepare for the future;
- Providing students and staff with the opportunity to personalize a student's education by combining rigorous academic study with the flexibility that is inherent in the anytime, anyplace philosophy; and
- Meeting the needs of a wide variety of students and fosters 21st Century skills such as global awareness, self-directed learning skills, information and communications technology literacy, problem-solving skills, and time management and personal responsibility.

Any use of VLACS's technology resources or network services by staff, other than for educational purposes, is not permitted.

Introduction:

The purpose of this policy is to state VLACS's guidelines for acceptable use of its technology resources and network services for educational purposes. This policy provides the procedures, rules, guidelines and the code of conduct for use of VLACS's technology resources, network services, and the Internet. These guidelines are a practical and logical extension of VLACS's commitment to conduct that is legal, ethical, and considerate.

For the purpose of this policy, "staff" and "users" refer to VLACS's employees, contracted service personnel, and any volunteers working within VLACS or these individuals who are working on behalf of VLACS in other schools.

VLACS's "technology resources" consist of all software, media, computers, printers and other peripheral devices that are owned or leased by VLACS. Any technology resource not owned or authorized by VLACS is not allowed to access VLACS's network services or the Internet without prior authorization from VLACS's Director of Instruction or his/her designee. Any computer, peripheral device, personal digital assistant, cell phone, pager or other device not owned by VLACS which has been specifically permitted to access VLACS technology resources or network services shall be governed by this policy and is considered a technology resource.

VLACS's "network services" consists of any configuration of hardware and software, which connects users to VLACS's network, other computers, peripheral devices, contracted software as service (SAAS) or the Internet. Network services include the computer hardware, operating system software, application software, stored text and data files, or any other device or application that allows or assists in the transfer of data within the network or to and from the Internet. Network services also include all devices that allow for the monitoring, security, and overall maintenance of VLACS's network.

Policy:

It is the policy of VLACS to maintain an environment that promotes ethical and responsible conduct by staff in all on-line and/or network activities. It is a violation of this policy for any user to engage in any activity that does not conform to the established purpose for VLACS providing technology resources and network services or which violates the guidelines described in this policy. VLACS's network shall not constitute a public forum. The use of VLACS's technology resources and network services are a privilege, not a right. Only authorized users may access VLACS's technology resources and network services. Staff shall use VLACS's technology resources and network in a professional, responsible, and ethical manner. A user's disciplinary consequences for violations of this policy will be determined by school administration and, depending upon the severity of the offense, may include verbal or written warning or discipline, restriction or revocation of access, removal, being reported to authorities, financial restitution, and employment termination.

Use of VLACS's Website:

VLACS maintains a website on the Internet for the purpose of communicating events involving VLACS, staff, students, and parents. VLACS's website is for the purpose of conveying general information about the schools, upcoming events, curriculum, policies, and procedures. All information or material posted to the website must at all times meet the policies and standards of VLACS. The website is not a public forum for any non-VLACS events or organizations. VLACS uniformly prohibits any unauthorized hyperlinks from its website to other websites. Any unauthorized hyperlink is a violation of this policy, subject to disciplinary action.

At any time and without advance notice, VLACS reserves the right to monitor, access, modify, remove, review and/or retrieve the subject, content and appropriateness of any and all information stored or transmitted on VLACS's website, hyperlinks or web page attached to VLACS's website.

Software:

Employees may use only preapproved software or Internet based applications while performing their duties. Staff must advise the Director of Instruction or his/her designee and request review and authorization prior to use of unapproved software or Internet based applications. Contents of all approved software and internet based applications must be consistent with VLACS's policies, procedures, regulations, and local, state and federal laws.

A signed Student Data Privacy Agreement must be in place prior to the approval of any software or online service, except where the software or service includes security certifications deemed acceptable by the New Hampshire Department of Education, in lieu of the minimum standards under RSA 189:66. (See NH Department of Education Publication, May 5, 2020, and as updated.)

Student Information:

In order to maintain the safety of VLACS students, student work or materials, pictures of students, and any such other information that would allow for the identification of students, such materials or depictions will only be allowed upon VLACS's receipt of written permission from students and their parents or guardians. All information about students posted on VLACS's website will comply with VLACS's policy on student records, the Federal Family Education Rights and Privacy Act, and any other applicable state or federal law.

Damage:

It is the policy of VLACS that all users of VLACS's technology resources and network services are required to conduct themselves in an appropriate manner. All users should refrain from any activity that may damage any technology resource equipment (e.g., tampering with or removing wires or keyboards from computers and jamming power cords and network wires into the ports on the machines) or interfere with or damage network services (e.g., downloading software or other applications without prior approval). VLACS's technology resources and network services are costly to obtain and to maintain. The technology resources are complex electronic equipment intended for the use of all users who are responsible and respect the privilege of using such advanced equipment. Users who damage VLACS's technology resources or network services may be liable for any financial loss incurred by VLACS.

Security:

Every VLACS employee shall follow these security practices:

1. Every employee must complete annual data security training.
2. Student records shall be stored in Google Drive accounts assigned to VLACS employees.
    a. Files may temporarily be downloaded to a device hard drive during active work sessions.
    b. Google Drive preferences must be set to stream, not mirror.
    c. If files are no longer needed, they should be deleted, not stored.
3. VLACS will provide every employee with password manager software.

    a. Every VLACS employee will use the password manager to log in to and access VLACS digital resources. Employees may use the password manager to store their personal account information in the appropriate password manager vault.
    b. Employees must create strong passwords. Password strength will be identified by the password manager application.
    c. Employees shall not copy or reuse passwords. Passwords may be used once and not reused for additional websites or software applications.
    d. Employees shall not share passwords with the following exceptions:
        i. Technology department staff or administrators may create temporary passwords for students or employees.
        ii. Employees may share passwords to software systems with limited account access using the school's password manager. This is allowed if it does not violate copyright rules.
    e. Passwords shall be stored only in the school's password manager.
    f. If an employee suspects that their user account or password has been compromised, it shall be reported immediately to the Technical Helpdesk or to a supervisor/administrator.
    g. Employees are required to change passwords at least one time per year.
2. Laptops assigned to VLACS employees will be equipped with a password manager and malware protection. Updates to these units will be administered remotely by VLACS technical staff or a contractor hired by VLACS.
3. VLACS employees who use personal technology to access VLACS digital resources must install and utilize the following security applications and/or configurations:
    a. Password manager purchased by VLACS
    b. Malware protection purchased by VLACS. This requirement is waived if the employee can provide evidence of the purchase and use of malware protection. Free versions of malware protection software are not acceptable.
    c. Personal technology shall be password protected with a strong password.
    d. If family members or friends will have access to personal technology that is used for VLACS work, the employee shall configure the unit to accommodate multiple users and separate the employee's account and associated data from other users.
    e. It is strongly recommended that hard drives be encrypted to prevent data from being accessed should the unit be lost or stolen.

Examples of Acceptable Uses of the VLACS's Technology Resources and Network Services are:

1. Communicating with students and other VLACS instructors or administrators
2. Purposes consistent with the educational objectives of VLACS
3. Tasks essential to school/VLACS administrative and communication needs
4. Assisting or supervising students with their on-line educational goals

Examples of Unacceptable Uses of VLACS's Technology Resources and Network Services may include but are not limited to:

1. Interfering with the work of a faculty member or school operations
2. Involvement in any activity that is prohibited by this policy or by any applicable law
3. Engaging in non-academic endeavors
4. Accessing an inappropriate website
5. Using for personal, financial or commercial use(s)
6. Participating in a public forum(s), "blogging," "chat rooms," or instant messaging
7. Sending, receiving or displaying offensive messages or pictures
8. Using obscene language
9. Harassing, insulting or attacking others
10. Cyber-bullying
11. Damaging or altering either VLACS or third party computers, computer systems, computer networks, peripheral devices, software or data
12. Violating copyright law or license agreements
13. Plagiarizing or cheating
14. Gaining access to or attempting to modify employees', teachers', students' or other third parties' folders, work or files
15. Gaining unauthorized access to restricted resources or organizations
16. Wasting limited resources, including bandwidth, server space, or printers
17. Using VLACS's network/Internet connection for any illegal or restricted activity
18. Participating in any scheme to defraud or unlawfully obtain money or property from others
19. Spreading, creating or using invasive software, such as computer viruses, worms, or other detrimental technology
20. Misrepresenting oneself in any e-mail communication or while accessing the network
21. Accessing, using, or distributing another's login or password
22. Violating any rules of behavior as listed in school policies.
23. Damaging or tampering with any technology resource equipment or network services
24. Allowing third-party access to technology resources or network services without prior authorization of the school administration
25. Posting items to the Internet or on VLACS's website or other technology systems without proper administrative authorization and parental permission, if the posting relates to students.
26. Encrypting communications or files to avoid system security review
27. Unauthorized use, installation, downloading and or copying of software or files
28. Use that violates any of VLACS's policies
29. Following students through any social network, for example Twitter, Facebook, or Instagram.

Incidental Use:

As a convenience to VLACS employees, incidental use of VLACS hardware or internet access is permitted. The following restrictions apply:

1. Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.
2. Incidental personal use of school laptops or internet access is restricted to VLACS employees; it does not extend to family members or other acquaintances.
3. Incidental use must not result in direct costs to VLACS without prior approval of management.
4. Incidental use must not interfere with the normal performance of an employee's work duties.
5. No files or documents may be sent or received that may cause legal action against, or embarrassment to VLACS.
6. Storage of files within VLACS's information systems is not permitted.
7. All messages, files, and documents — including personal messages, files, and documents — located on VLACS information systems or hardware are owned by VLACS, may be subject to open records requests, and may be accessed in accordance with this policy.

Privacy:

Users have no right of privacy with regard to their use of VLACS's technology resources and network services, including but not limited to email, any data transferred over VLACS's network, accessing the Internet, information stored on VLACS computers or any other VLACS owned or leased data storage media. VLACS retains all ownership and possessory control of its technology resources and network services, along with all data stored therein.

While it is not the intent of VLACS personnel to be intrusive, VLACS reserves the right to monitor the use of technology resources and network services, and to monitor, access, review or retrieve any information transferred over the network or stored on VLACS computers or any other VLACS-owned data storage media or technology resource as defined in this policy. Users shall provide all passwords needed to access this information if requested by school administration.

As a school, VLACS is a public entity subject to laws regarding public records and their disclosure. Users must understand that all emails, Internet logs, and other VLACS documents and electronic records may be accessed by third parties, including Internet service providers, and may be the subject to disclosure upon a public records request or be disclosed to the general public under certain circumstances.

Copyrighted and Proprietary Materials:

All users shall respect the copyright and proprietary interests of owner's materials accessed through VLACS's technology resources and network services. Users may not copy or download from the Internet any software, including VLACS-owned software, without permission from the copyright holder, whether for personal use or other use because certain unauthorized duplication even for educational purposes may violate copyright law. VLACS recommends that if there is any question concerning the use of copyrighted material that users seek guidance from VLACS's Director of Instruction or his/her designee.

Limitation of Liability:

VLACS makes no warranties of any kind, whether express or implied for the service it is providing. VLACS will not be responsible for any direct or indirect, incidental or consequential damages suffered through the use, operation, or inability to use VLACS's technology resources or network services. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by VLACS's negligence or user errors or omissions. VLACS assumes no responsibility for the accuracy or quality of information obtained through the use of technology resources or network services, the Internet and any related technology.

VLACS will not be responsible for financial obligations arising through the unauthorized use of technology resources or network services.

Notification of Violations:

Staff should immediately notify the Director of Instruction
or his/her designee of any violations of this policy.

VLACS reserves the right to make individual written exceptions to the above restrictions upon requests to the network administration and to add further unacceptable uses as it deems appropriate to this policy.

Law Reference:
Appendix Reference:
Date Adopted: June 9, 2011,
Revision Dates: May 25, 2023, January 18, 2024