STUDENT CODE OF CONDUCT & ACCEPTABLE USE IJND

Introduction

The purpose of this Policy is to ensure the efficient, safe, ethical, and legal use of the VLACS Technology. This Policy applies to all student users of VLACS Technology, as well as users who obtain their access privileges through association with VLACS.

Student and Parent Acknowledgement

Every student and his/her parent must electronically acknowledge the existence of this policy as a condition to receive access to VLACS Technology. The Acknowledgement will remain in effect until such time as the student is no longer enrolled in VLACS courses or a policy revision requires that a new Acknowledgement form be reviewed.

Educational Purposes

The purpose of VLACS Technology is to serve as a resource for teaching and learning at VLACS. VLACS Technology, including approved Artificial Intelligence (AI) tools, may be used only for purposes consistent with the educational objectives of VLACS and in adherence to the VLACS Academic Integrity policy. VLACS Technology may not be used for recreational, personal, or commercial purposes unless explicitly permitted for educational activities.

Only authorized users may access VLACS Technology. VLACS Technology shall not constitute a public forum. VLACS students will have the ability to contact other VLACS students and employees via VLACS Technology. All communications and information accessible via any VLACS Technology may be accessed by VLACS and treated as VLACS property. This includes, but is not limited to, email, chat text, voicemail, and course-related documents or other files.

Users are responsible for ensuring that their activities adhere to generally accepted educational standards. Inappropriate use includes all those activities prohibited to the user based on their allowed degree of access and any activity that violates the school's policies or procedures.

Student Responsibilities may include but are not limited to:

- Students are responsible for good behavior when using VLACS Technology just as they are in a traditional school setting.
- Integrity and authenticity of student work is taken very seriously at VLACS. Do not cut, copy, or plagiarize Internet content or the work of your online classmates. VLACS instructors utilize technologies to check for authenticity. Copying, knowingly allowing others to copy from you, and/or misusing Internet content could result in removal from VLACS courses.
- Integrity and authenticity of student work are essential at VLACS. Students must adhere to Policy JIC (Academic Integrity). Violations of this policy, including undisclosed AI-generated content, could result in removal from VLACS courses.

- Always use show consideration and respect for others when using VLACS Technology
- Communications with VLACS classmates should be course-related.

Unacceptable Uses of VLACS Technology may include but are not limited to:

- Accessing, storing, or sending an inappropriate or indecent website, files, messages, or images.
- Cyber-bullying or using obscene language, harassing, insulting, defaming, threatening or attacking others
- Using Artificial Intelligence (AI) tools to create, disseminate, or manipulate media (e.g., deepfakes, synthetic audio or video) for the purpose of harassment, bullying, intimidation, misinformation, or any other malicious or deceptive intent targeting individuals or groups, as further detailed in VLACS Policy JICL (Pupil Safety and Violence Prevention).
- Entering Personally Identifiable Information (PII), confidential data, or sensitive information about students, staff, or VLACS operations into any AI tool that has not been formally approved by VLACS and is not on the "Approved AI Tools List."
- Using AI to generate, access, or distribute content that is illegal, sexually explicit, violent, harassing, hateful, discriminatory, or otherwise inappropriate for a K-12 educational setting.
- Using AI to impersonate another student, staff member, parent, or any individual without explicit permission and clear, documented educational justification.
- Transmission of unsolicited advertising, promotional materials, or other forms of solicitation, including placing hyperlinks to non-VLACS related web sites
- Mass mailings within VLACS without receiving permission from the Director of Technology
- Gaining access to or attempting to modify employees', instructors', students' or third parties' folders, work or files
- Gaining unauthorized access to restricted resources or organizations
- Using AI tools to bypass VLACS's security measures, gain unauthorized access to restricted resources, or engage in any form of cyber-attack or malicious activity.
- Spreading, creating or using invasive software, such as computer viruses, worms, malware, or other detrimental technology
- Misrepresenting oneself in any e-mail communication or while accessing VLACS Technology
- Allowing third-party access to VLACS Technology without prior authorization from the Director of Technology or Chief Executive Officer
- Encrypting communications or files to avoid security review
- Accessing, using, or distributing another user's login or password
- Sharing personal passwords or personal information, or mishandling passwords, access codes or other data in violation of any VLACS policy
- Inappropriate activities performed through a student's account will be considered to be the actions of the account holder.
- Involvement in any activity that is prohibited by this Policy, other VLACS policies, or by applicable law

Students should immediately notify their instructor, or the VLACS office of any violations of

this Policy.

VLACS reserves the right to make individual written exceptions to the above restrictions upon requests to the Chief Operating Officer or Chief Executive Officer, and to add further unacceptable uses as it deems appropriate to this Policy.

Personal Security

In addition to following the acceptable use guidelines listed above, VLACS recommends the following rules when students are outside VLACS' online learning environment:

- Never arrange to get together with someone "met" online, unless you have parental permission.
- Do not respond to any illicit or suspicious activities, and immediately report them to a school administrator.
- Do not engage in any activity that may violate VLACS' Pupil Safety and Violence Prevention Policy JICL.
- Beware of emails from anyone, particularly adults you do not know, asking for personal information, attempting to arrange meetings, or engaging in personal contact.
- Alert your instructor or other Virtual Learning Academy Charter School employee of any message you receive that is inappropriate or makes you feel uncomfortable.
- Never say anything via email that you would not mind seeing in a local newspaper.
- Be cautious when interacting with Artificial Intelligence (AI) tools outside of VLACS's approved list, especially regarding the input of personal or sensitive information. Understand that data shared with unvetted AI models may not be private.
-

VLACS cannot guarantee the appropriateness or accuracy of the information that students may access on the Internet outside of VLACS Technology. For those students who access VLACS Technology from a home computer, parents should be aware of this and monitor their children's communications and use of the Internet. Parents/guardians and students should review the information and documents available on the NH Attorney General's website at: https://www.doj.nh.gov/criminal/internet-safety.htm.

Children's Online Privacy Protection Act (COPPA)

COPPA is a federal law that applies to the collection of personal information from children under 13 years of age. COPPA prohibits commercial website operators who operate websites directed towards children from gathering personally identifiable data on children under age 13. VLACS is not a commercial website operator and it will not be liable under COPPA. Parents should reference VLACS' Family Educational Rights and Privacy Act Annual Notice to understand what information may be collected and disclosed by VLACS to third party vendors who contract with VLACS.

VLACS is committed to ensuring that all Artificial Intelligence (AI) tools and services utilized, especially those interacting with student data, comply with COPPA, FERPA, and all other applicable data privacy laws.

Consequences for Violation of the Policy

Access to the Technology is a privilege, not a right. Users who abide by this Policy will be allowed to access VLACS Technology and any other technological resources made available to them. Users who do not abide with the policies set forth herein may be denied access to the Technology. Also, failure to abide by this Policy could also lead to discipline, up to and including expulsion, and a report to the police concerning any violation of the law. Acceptable use practices, policies, and guidelines apply to anyone who accesses VLACS Technology.

VLACS' Rights

VLACS Technology is maintained and managed by the Director of Technology in such a way as to ensure its availability and reliability in performing its educational mission. Users have no reasonable expectation of privacy concerning any materials transferred over or stored with VLACS Technology, even if protected by password.

The VLACS reserves the right to:

- Monitor all activity and use of VLACS Technology
- Make determinations on whether specific uses of VLACS Technology are consistent with this Policy
- Log Technology used by users
- Determine what is an appropriate use
- Remove user access to VLACS Technology at any time it is determined that the user engaged in unauthorized activity or violated this Policy
- Any VLACS administrator may terminate the account privileges of a student for any reason.
- Cooperate fully with any investigation and law enforcement concerning or relating to VLACS Technology activity.

Definition and Scope of VLACS Technology

VLACS Technology consists of all on-line computer accounts and applications owned or leased by VLACS, and any configuration of computer hardware and software that connects the users to the Technology. The term includes all internal (intranet) and external (internet) connections as well as all of the computer hardware operating systems software, application software, stored text, and data, voice, and image files. The term also includes computer accounts, electronic mail, local databases, externally accessed databases, DVD, digitized information, communication technologies and new technologies as they become available. This definition explicitly includes all Artificial Intelligence (AI) tools, platforms, and models utilized by VLACS or accessed through VLACS Technology.

Any computer, peripheral device, tablet computer, cell phone, pager or other device, not owned by VLACS, but which has been permitted to access the Technology, or which accesses the Technology without permission shall be governed by this Policy.

VLACS' Limitation of Liability

VLACS makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through VLACS Technology will be error-free or without defect.

VLACS will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. VLACS is not responsible for the accuracy or quality of the information obtained through or stored on the system. VLACS will not be responsible for financial obligations or repair costs arising from the unauthorized use or intentional misconduct. VLACS assumes no responsibility for any phone charges, line costs or usage fees for connectivity to the Internet.

Law References:
RSA 194:3-d, School District Computer Networks
47 U.S.C. Section 254, Children's Internet Protection Act, Effective April 20, 2001
15 U.S.C. Section 6501-6506, Children's Online Privacy Protection Act

References:
Federal Trade Commission website for information about COPPA - http://business.ftc.gov/privacy-and-security/children%E2%80%99s-privacy

Date Adopted: January 3, 2008

Revision Dates: November 15, 2012, March 17, 2016, September 25, 2025