VIRTUAL LEARNING ACADEMY CHARTER SCHOOL POLICY

DATA SECURITY AND PRIVACY **EHAB**

The provisions of this Virtual Learning Academy Charter School, hereinafter referred to as VLACS, policy shall supersede and take precedence over any contrary provisions of any other policy adopted prior to the date of this policy.

A. Definitions

1. Public Data: Information that is intended for or may be released to the general public without restriction. This includes "Directory Information" as defined in policy JRA, Student Records – FERPA including, but not limited to, student name, participation in sports, and honors/awards; school calendars; and public announcements.

2. Confidential Data: Information protected by federal or state law, regulations, or legal contracts that requires strict access controls. This is sensitive data. It includes, but is not limited to, non-directory Student Records such as grades, transcripts, and disciplinary files; Special Education records including, but not limited to, IEPs; and employee personnel files.

3. Restricted Data: Highly sensitive information that is not necessarily academic but poses a high risk of identity theft or financial loss if exposed. This includes, but is not limited to, data such as Social Security numbers, driver's license numbers, government identification numbers, financial account details, login credentials including, but not limited to, passwords and hashes, and biometric data.

4. Critical Data: Information that is determined to be essential to VLACS' operations and that must be accurately and securely maintained to avoid disruption to VLACS' operations. Critical data is not necessarily confidential.

5. Network Services: The entire ecosystem of hardware, software, and infrastructure that enables data transmission and connectivity. This includes, but is not limited to, physical servers, routers, and cables, as well as the invisible layers like operating systems, cloud applications, and monitoring tools used to maintain security and performance.

6. Security Breach: Any incident—intentional or accidental—that results in the unauthorized access, disclosure, modification, or destruction of Confidential or Restricted data.

7. Personally Identifiable Data: Data from educational records that can be used to distinguish or trace a student's identity, either directly or indirectly by linking other information to it. Examples include names, birthdays, social security numbers, and addresses.

B. Data and Privacy Governance Plan - Administrative Procedures

1. Data Governance Plan

The Chief Executive Officer, hereinafter referred to as the CEO, in consultation with the Information System Security Officer, hereinafter referred to as the ISSO and further defined in paragraph C below, shall create a Data and Privacy Governance Plan, referred to as the Data Governance Plan, to be presented to the Board no later than June 30, 2019. Thereafter, the CEO, in consultation with the ISSO, shall update the Data Governance Plan for presentation to the Board no later than June 30 each year.

The Data Governance Plan shall include:

(a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use;

(b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;

(c) Policies and procedures for access to data and protection of privacy for students and staff including, but not limited to, acceptable use policy for applications, digital tools, and extensions;

(d) A response plan for any breach of information; and

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2. Policies and Administrative Procedures

The CEO, in consultation with the ISSO, is directed to review, modify and recommend policies and create administrative procedures, where necessary, relative to collecting, appropriately securing, and correctly disposing of VLACS data including, but not limited to, public data, confidential data, restricted data, critical data, and personally identifiable data, and otherwise as necessary to implement this policy and the Data Governance Plan. Such policies and/or procedures may or may not be included in the annual Data Governance Plan.

3. Software List

VLACS maintains a list of approved software applications that meet Minimum Standards as established under RSA 189:66, Student and Teacher Information Protection and Privacy, on this webpage: https://sdpc.a4l.org/district_listing.php?districtID=8280

C. Information Systems Security Officer

The VLACS Information Systems Security Officer hereinafter referred to as the ISSO, reports directly to the CEO or their designee. The ISSO is responsible for supervising the implementation and enforcement of the VLACS' Data Governance Plan, security policies and administrative procedures applicable to digital and other electronic data. Additionally, the ISSO

is responsible for suggesting changes to policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of VLACS' data. The ISSO will work closely with the technology team and the administrative team to advocate for resources and training to best secure VLACS' data.

D. Responsibility and Data Stewardship

All VLACS employees, contractors, volunteers, and agents are responsible for accurately collecting, maintaining and appropriately securing data including, but not limited to, public data, confidential data, restricted data, critical data, and personally identifiable data.

E. Data Managers

All members of the VLACS administrative team are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the school's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the school and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISSO in enforcing school policies and procedures regarding data management.

F. Confidential, Restricted, and Critical Information

VLACS will collect, create or store confidential and restricted information only when the CEO or their designee determines it is necessary and in accordance with applicable law. VLACS will provide access to confidential and restricted information to appropriately trained VLACS employees, contractors, volunteers, and agents only when VLACS determines that such access is necessary for the performance of their duties. VLACS will disclose confidential and restricted information only to authorized contractors or agents who need access to the information to provide services to VLACS and who agree not to disclose the information to any other party except as allowed by law and authorized by VLACS. VLACS employees, contractors, volunteers, and agents will notify the ISSO or their designee immediately if there is reason to believe confidential or restricted information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. Policy EHA, Data Breach, will provide guidance in such situations. Likewise, VLACS will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed, or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure. All VLACS staff, contractors, volunteers, and agents who are granted access to confidential, restricted, or critical data are required to keep the data secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such confidential, restricted, or critical data. All individuals using confidential, restricted, critical data, or personally identifiable data will strictly observe all administrative procedures, policies, and other protections put into place by VLACS including, but not limited to, maintaining information

in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information no longer needed in a confidential and secure manner.

G. Using Online Services and Applications

VLACS staff members are encouraged to research and recommend online services or applications to engage students and further the VLACS' educational mission. VLACS employees, however, are prohibited from installing or using applications, programs or other software, or online system/website, that either stores, collects, or shares confidential, restricted, or critical data until the CEO or designee and ISSO or designee approve the vendor and the software or service used. Before approving the use or purchase of any such software or online service, the ISSO or designee shall verify that it meets the requirements of the law, Board policy, and the Data Governance Plan and that it appropriately protects confidential, restricted, and critical data/information. This prior approval is also required whether or not the software or online service is obtained or used without charge.

H. Training

The ISSO or designee will provide appropriate training to employees who have access to confidential, restricted, critical information, or personally identifiable data to prevent unauthorized disclosures or breaches in security. All VLACS employees will receive annual training in the confidentiality of student records, the requirements of this policy, and related procedures and rules.

I. Data Retention and Deletion

The ISSO or designee shall establish processes and procedures following the retention schedule established in Policy EHB-R for the regular archiving and deletion of data stored on VLACS technology resources, including but not limited to, provisions relating to Litigation and Right to Know holds as described in Policy EHB-R.

J. Consequences

Employees who fail to follow the law or VLACS policies or procedures regarding data governance and security including, but not limited to, failing to report may be disciplined, up to and including termination. Volunteers may be excluded from providing services to VLACS. VLACS may end business relationships with any contractor who fails to follow the law, VLACS policies or procedures, or the confidentiality provisions of any contract. In addition, VLACS reserves the right to seek all other legal remedies, including, but not limited to, criminal and civil action and seeking discipline of an employee's teaching certificate. VLACS may suspend all access to data or use of VLACS technology resources pending an investigation. Violations may result in temporary, long-term, or permanent suspension of user privileges. VLACS will

cooperate with law enforcement in investigating any unlawful actions. The CEO or designee has the authority to sign any criminal complaint on behalf of VLACS.

Any attempted violation of VLACS policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

Legal References:

15 U.S.C. §§ 6501-6506 * Children's Online Privacy Protection Act (COPPA)
20 U.S.C. § 1232g * Family Educational Rights and Privacy Act (FERPA)
20 U.S.C. § 1232h * Protection of Pupil Rights Amendment (PPRA)
20 U.S.C. § 1400-1417 * Individuals with Disabilities Education Act (IDEA)
20 U.S.C. § 7926 * Elementary and Secondary Education Act (ESSA)
34 C.F.R. § 99.3, Personally Identifiable Info
RSA 189:65 * Definitions RSA 186:66 * Student Information Protection and Privacy
RSA 189:67 * Limits on Disclosure of Information
RSA 189:68 * Student Privacy RSA 189:68-a * Student Online Personal Information
RSA 359-C:19-21 * Right to Privacy/Notice of Security Breach

Legal References Disclaimer:

These references are not intended to be considered part of this policy, nor should they be taken as a comprehensive statement of the legal basis for the Board to enact this policy, nor as a complete recitation of related legal authority. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

Date Adopted: May 23, 2019

Revision Dates: May 20, 2021; September 16, 2021; May 26, 2022; January 19, 2023; May 5, 2026

Last Review Date: May 5, 2026