Vista Higher Learning Data Security and Privacy Plan

Vista Higher Learning's ("VHL", "VHL's", "We", "Our") objective, in the development and implementation of this Data Security and Privacy Plan ("Plan"), is to create effective administrative, technical and physical safeguards for the protection of student data ("Student Data") collected from our institutional customers, and to comply with obligations under applicable data security and privacy laws, such as New York State Education Law 2-d.

For purposes of this Plan, "Student Data" means personally identifiable information from student records of an educational agency, as defined in New York State Education Law 2-d or other state law applicable to our institutional customers. In addition, VHL is committed to protecting the confidentiality of all sensitive data that it maintains, and we have implemented a number of policies to protect such information, including our Written

Information Security Program (WISP), provided on written request at privacyrequest@vistahigherlearning.com, and our Privacy Policy, found at https://www.vhlcentral.com/privacy_policy. Our Plan should be read in conjunction with these policies.

1. Purpose:

The purpose of this Plan is to:

- Ensure the security and confidentiality of Student Data;
- Protect against any anticipated threats or hazards to the security or integrity of such Student Data;
- Protect against unauthorized access to or use of such Student Data.

2. Scope:

In formulating and implementing the Plan, we (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of records containing Student Data; (2) assess the likelihood and potential damage of these threats; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to

control risks; (4) design and implement a Plan that puts safeguards in place to minimize those risks, consistent with the requirements of New York State Education Law 2-d and other state law applicable to our institutional customers; and (5) regularly monitor the effectiveness of those safeguards.

3. Data Security:

Data Security Team

VHL has designated a Data Security Team, led by the Executive Vice President of Technology and consisting of the CEO, senior departmental leadership, and data and security leadership. This Data Security Team shall be responsible to:

- Implement the Plan;
- Provide appropriate training or otherwise ensure that appropriate training occurs for all owners, managers, employees, and independent contractors with access to Student Data in a manner consistent with the requirements of the Plan, as follows:
    - Mandatory annual training by functional area for all owners managers, employees and contractors with access to student PII

- Mandatory onboarding training via recorded video for all new employees
- The training covers the following topics:
    1. VHL Oversight: Introduction to the Data Security Team
    2. Confidential Data Laws, Policies and Agreements
    3. Confidential VHL Business Data
    4. Personally Identifiable Customer Data
    5. The Top Responsibilities to Protect Confidential Data
    6. Know how to protect confidential data, and make sure others do too.
    7. Collect and retain only what confidential data is needed.
    8. Protect who has access to confidential data.
    9. Protect the confidential data you use.
    10. Protect how you access and use the confidential data you use.
    11. Protect the business systems that protect the confidential data you use.

12. Never share confidential data outside of the VHL business.
13. Understand customer rights to their data.
14. Confidential customer data is never for sale.

- As appropriate, monitor and test the Plan's safeguards;
- Require third party service providers with permitted access to Student Data by contract to implement and maintain appropriate security measures for Student Data;
- Perform a review of the Plan no less than annually.

4. Compliance with District's Parents' Bill of Rights Regarding Data Privacy and Security:

VHL has implemented commercial and technical practices within its policies and practices that comply with the District Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to VHL's possession and use of Student Data pursuant to District contracts and written agreements.

5. Data Accuracy and Collection Practices:

A parent, student, teacher, or principal may challenge the accuracy of data by contacting VHL or the District. VHL will notify District of any challenges to the accuracy of data, and the District will then handle the challenges with the parent, student, teacher or principal as necessary. In the event that District notifies VHL of the outcome of any such errors made by VHL, VHL will promptly correct any inaccurate data it or its subcontractors or assignees maintain.

6. Compliance with State and Federal Data Security and Privacy Protections:

VHL has implemented commercial and technical policies and practices that comply with all applicable provisions of State and Federal laws, including Family Educational Rights and Privacy Act, 20 USC 1232g, and its regulations, 34 CFR Part 99 (“FERPA”), Children's Online Privacy Protection Act of 1998, 15 USC 6501–6508, and New York State Education Law 2-d and other state laws applicable to our institutional customers, in collecting and processing Student Data. VHL agrees to use Student Data only for educational purposes. Student Data is, and will continue to be, property of and under the control of the District.

7. Internal and External Controls to Protect the Privacy of Student Data:

To combat the internal and external risks to the security, confidentiality, and/or integrity of Student Data, VHL employs the following technical and commercial practices:

Measures

- VHL shall only collect Student Data in an amount that is reasonable to accomplish legitimate business purposes or necessary to comply with other state and federal regulations;
- VHL shall limit access to Student Data to those persons who need it to accomplish a legitimate business purpose or otherwise comply with other state or federal regulations;
- VHL shall use Student Data solely for the purpose of providing services as set forth in contracts or written agreements between VHL and District;
- Except for authorized representatives of the third party contractor to the extent necessary to accomplish a legitimate business purpose, VHL shall not disclose any personally identifiable information to any other party;

- VHL shall not sell or use for targeted marketing purposes Student Data.
- VHL shall use encryption no less stringent than the following to encrypt Student Data in transit and at rest, respectively: TLS 1.2 and AES 256;
- VHL shall store all Student Data within secure hosting centers within the United States. For the sake of clarity, VHL uses US-based Amazon Web Services (AWS) cloud hosting centers;
- When contracts or written agreements expire, VHL shall securely delete Student Data as mutually agreed in such contracts or written agreements, and otherwise upon the written request of the District;
- VHL shall ensure that electronic access to and use of Student Data requires the following:
    - Secure user authentication, access and use protocols, including:
        15. Unique user IDs;
        16. Reasonably secure methods for assigning and securing passwords;
        17. Controls, including encryption, for storage of passwords;

18. Restricted access to active users and user accounts only;

19. Prompt removal of access for terminated employees or other persons no longer required to have access;

20. Access blocks to user logins after multiple unsuccessful attempts to gain access or the limitations placed on access for a particular system;

21. Mandatory timed system timeouts that require user to re-enter their username and password.

- Secure access control measures that:

    1. Restrict access to records and files containing Student Data to those who need such information to perform their job duties;

    2. Assign unique User IDs and passwords, which are not vendor supplied default passwords, to each person with computer access;

    3. Reasonably monitor systems for unauthorized use of or access to Student Data;

4. Maintain up-to-date firewall configurations, operating system security updates and patches, and malware and virus protections; and

5. Securely destroy or erase data on de-commissioned storage drives and hardware such as to render any Student Data unreadable and unable to be reconstructed.

- All VHL employees, vendors and independent contractors with access to Student Data shall:
    - Abide by the terms of this Data Security and Privacy Plan, in accordance Education Law §2-d;
    - Sign confidentiality agreements ensuring necessary Student Data protections;
    - Receive appropriate training on the requirements and safeguards of the Plan;
- VHL shall maintain and operate appropriate incident response and investigation processes and procedures ("Incident Response") in the event that suspicious or unauthorized access and use of Student Data is discovered or otherwise reported to the Data Security Team. The Incident Response process shall include the following:
    - Prompt steps to mitigate the access, evaluate and respond to the events, notify users affected by the

access, and engage appropriate auditors or examiners in connection with the access, subject to reasonable notice, access and confidentiality limitations.

- In the event that an unauthorized release of Student Data by VHL or its assignees occurs, VHL shall notify District in the most expedient way possible and without unreasonable delay;
- VHL shall adopt security policies that align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework;
- VHL shall follow SOC 2 Type 2 security protection practices and undergo annual audits of those practices by expert external auditing firms.

`Version Effective 6-21-2024`