Heritage Heights Academy's Student Data Privacy Policy

1. Overview

Student data security and privacy, and public confidence in the same, is a critical component of Heritage Heights Academy's (School) ability to make informed, data-supported educational decisions that impact the lives of students. The safe collection, use, protection, and management of the various types of student Personally Identifiable Information (PII) or other sensitive data is critical to School operations. School information collecting systems should generally only collect and record student data for purposes related to student education, school management, reporting, or other appropriate, school-related purposes. Student PII or other sensitive data requested, collected, captured, generated, stored, or otherwise entrusted to and maintained by School should be shared only for legitimate educational purposes with those who are authorized, or as required by law. Reasonable care must be taken to ensure that Student PII or other sensitive data is never misused or disclosed to unauthorized individuals.

2. Definitions

For purposes of this policy, the following definitions apply:

"Aggregate data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

"Data" means any student or family information collected, captured, stored, generated, or otherwise entrusted to and maintained by School, its employees, contractors, agents, systems, storage devices, or other means. This includes systems and devices involved in the transmission and storage of video and voice data.

"Data Security Breach" or "Breach" is any occurrence that results in School or an SSCP being unable to put in place controls or take other action to reasonably prevent the unauthorized disclosure or misuse of sensitive data or student PII. A Data Security Breach or Breach is also any occurrence of unauthorized disclosure or misuse of sensitive data or student PII, whether it be internal or external and/or unintentional or intentional.

"Destroy" means to remove student personally identifiable information so that it is permanently irretrievable in the normal course of business.

"Parent" means a student's biological or adoptive parent or the student's legal guardian.

“Student Personally Identifiable Information” means any data that, alone or in combination, would allow a reasonable person to determine or infer the personal identity of a student or the student’s parents or family in relation to the other information contained in the data.

“School service” means an internet website, online service, online application, or mobile application that is designed and marketed primarily for use in a preschool, elementary school, or secondary school; is used at the direction of teachers or other employees of School; and collects, maintains, or uses student personally identifiable information. “School service” does not include an internet website, online service, online application, or mobile application that is designed and marketed for use by individuals or entities generally, even if it is also marketed to a United States preschool, elementary school, or secondary school.

“School service contract provider” (SSCP) means an entity, other than a public education entity or an institution of higher education, that enters into a formal, negotiated contract with School to provide a school service.

“School service on-demand provider” (SSODP) means an entity, other than a public education entity, that provides a school service on occasion to School, subject to agreement by School, or an employee of School, to standard, non-negotiable terms and conditions of service established by the providing entity.

“Sensitive” or “Confidential” means data that is deemed confidential by law, or any data for which the student or family to whom the data relates would have a reasonable expectation of privacy, and the unauthorized sharing of which would reasonably be considered an invasion of privacy or harmful.

“Student Data Transparency and Security Act” (SDTSA) refers to the law as it now exists or may be amended in Colorado Revised Statutes 22-16-101, et. seq.

“Targeted advertising” means selecting and sending advertisements to a student based on information obtained or inferred over time from the student's online behavior, use of applications, or personally identifiable information. “Targeted advertising” does not include advertising to a student at an online location based on the student's current visit to that location or in response to the student's request for information or feedback, and without the collection and retention of a student's online activities over time; adaptive learning, personalized learning, or customized education; or with the consent of a student or the student's parent, using the student's personally identifiable information to identify for the student institutions of higher education or scholarship providers that are seeking students who meet specific criteria.

3. Purpose

This policy establishes requirements and guidelines for School to follow with regards to student data privacy and security. This policy attempts to be as comprehensive as possible, but it is not intended to cover every situation or to be an adequate replacement for developing additional procedures and practices for carrying out the requirements and guidelines of this policy on a day-to-day basis.

This policy is designed to meet the requirements for School to adopt a student data privacy and security policy pursuant to Colorado's Student Data Security and Transparency Act, as delineated in C.R.S. 22-16-107(4)(a).

4. Policy

A. General Statement

Using data effectively and responsibly is foundational to making the best decisions in today's schools and improving student performance. School has an interest in ensuring that it is a trusted partner when collecting data from students and families. At all times School will follow all applicable federal and state laws related to data privacy, including the federal Family Educational Rights Privacy Act (FERPA) and Colorado's Student Data Transparency and Security Act (SDTSA).

School student data privacy procedures and practices must be designed to adhere to requirements set forth in applicable federal and state law. In general, these procedures and practices should include additional safeguards as follows:

- A specific review of out-of-the-ordinary requests for student PII or sensitive data by School Executive Director and legal counsel;
- Regular review of student data privacy policies, procedures, processes and practices by School Executive Director and Board of Directors, with input from legal counsel and other experts in the field of data security to ensure that it remains current and adequate to protect student PII in light of advances in applicable law, as well as data technology and dissemination;
- Specific language must be included in vendor/contractor agreements that bind them to follow applicable laws, and also the policies, procedures, and processes developed by School to protect student data privacy;
- School must undergo regular, independent security audits;

- A record must be maintained for out-of-the-ordinary requests and releases of student data.

B. Uses of Student PII

Student PII or other sensitive data may be collected, used, maintained, disclosed, and reviewed by School and staff only for legitimate educational purposes related to educational decisions, legal compliance, reporting, or other lawful purposes.

In general, no Student PII or other sensitive data will be shared with third parties outside of legally compliant activities or as specifically authorized by law, unless that release of data is authorized by the parent or student of majority age.

School will only provide student PII to the Colorado Department of Education as required by state or federal law; except that it may provide student PII not mandated by state or federal law if it is associated with a grant proposal, or as a condition of receiving a benefit, such as grant funding or special designations. Unless required by state or federal law, School will not provide the following: juvenile delinquency records; criminal records; medical and health records; student social security numbers; student biometric information; and information concerning the political affiliations or the beliefs or attitudes of students and their families.

To ensure clarity, this policy is not intended to prohibit the use of student PII to: use adaptive learning or design personalized or customized education; maintain, develop, support, improve, or diagnose an SSCP's website, online service, online application, or mobile application; provide recommendations for school, educational, or employment purposes within a school service, so long as the response is not determined in whole or in part by payment or other consideration from a third party; respond to a student's request for information or for feedback so long as the information or response is not determined in whole or in part by payment or other consideration from a third party; identify for the student, only with the written consent of the student or the student's parent, institutions of higher education or scholarship providers that are seeking students who meet specific criteria, regardless of whether the identified institutions of higher education or scholarship providers provide consideration to the SSCP; in accordance with the terms of a contract between the SSCP and School, produce and distribute, free or for consideration, student class photos and yearbooks only to the public education entity, students, parents, or individuals authorized by parents; or provide for the student, only with the express written consent of the student or the student's parent given in response to clear and conspicuous notice, access to employment opportunities, educational scholarships or financial aid, or postsecondary education opportunities, regardless of whether the SSCP receives consideration from one or more third parties in exchange for the student personally identifiable information, so long as the SSCP provides a nationally recognized assessment that postsecondary institutions of higher education use in making admissions decisions.

Further, this policy is not intended to: impede the ability of a student to download, export, or otherwise save or maintain his or her own student personally identifiable information or documents; limit internet service providers from providing internet connectivity to School or to students and their families; prohibit an SSCP from marketing educational products directly to parents so long as the marketing does not result from the use of student PII obtained by the SSCP as a result of providing its website, online service, online application, or mobile application; or impose a duty on a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this article on that software or those applications.

C. Maintaining, Retaining and Destroying Student PII

School will post and regularly update on its website clear information that is understandable by a layperson listing the data elements of student PII it collects and maintains in its data system, except it will not include the student PII it collects and transmits to the Colorado Department of Education. The list will explain how School uses and shares the student PII. School will also include a link to the data inventory and dictionary or index of data elements that the Colorado State Board of Education is required to publish.

A student's parent, upon request, must be allowed to inspect and review his or her child's student PII maintained by the local education provider. A student's parent, upon request, must be provided a paper or electronic copy of his or her child's student PII, including student PII maintained by an SSCP. If a parent requests an electronic copy School shall provide an electronic copy unless School does not maintain that student PII in electronic format and reproducing the student PII in an electronic format would be unduly burdensome.

A student's parent may request corrections to factually inaccurate student PII maintained by School. After receiving a request for correction that documents the factual inaccuracy, School must determine if a factual inaccuracy exists and, if it does exist, it must correct the factual inaccuracy and confirm the correction to the parent within a reasonable amount of time. If a parent disagrees with the decision not to correct a factual inaccuracy, they may file a complaint pursuant to section G of this policy.

School uses the School Districts Records Management Manual published by the Colorado state archivist as a guideline for determining the length of time for retaining student records and PII. Once it is determined that a student record or PII will no longer to be retained, it must be immediately and thoroughly destroyed, as that term is defined in this policy.

During the term of a contract between an SSCP and School the SSCP must contractually agree to destroy, as soon as practicable, a student's PII collected, generated, or inferred as a result of the contract, at the request of School, unless the

SSCP obtains the consent of the student or the student's parent to retain the student's PII, or the student transfers to another public education entity and the receiving public education entity requests that the SSCP retain the student's PII.

Any SSCP must contractually agree to, following the termination or conclusion of the contract, destroy all student PII collected, generated, or inferred as a result of the contract. If the contract does not specify a period for destruction of the student PII, the SSCP must destroy the information when the information is no longer needed for the purposes described in the contract. The contract provider shall notify School of the date upon which all of the student PII is destroyed.

School will follow these data disposal procedures:

All computer desktops, laptops, hard drives, and portable media must be processed through the IT department for proper disposal. Paper and hard copy records containing student PII or other sensitive data shall be disposed of in a secure manner (shredding, incineration, etc.).

The Executive Director will work with the IT Department to ensure procedures exist and are followed to:

1. Address the evaluation and final disposition of student PII or other sensitive data found on hardware or electronic media regardless of media format or type.

2. Specify a process for making sensitive information unusable and inaccessible. These procedures should specify the use of technology (e.g. software, special hardware, etc.) or physical destruction mechanisms to ensure sensitive information is unusable, inaccessible, and unable to be reconstructed.

3. Determine the authorized personnel who will be responsible to dispose of student PII or sensitive data found on equipment of electronic media.

D. Student PII Security Breaches

If it is determined that a student data security breach has occurred, School will immediately notify those students and parents who are known to be affected by the breach. If the full scope of the breach is not certain, School will notify all students and parents who are potentially affected by the breach. School must take immediate measures to contain the breach and remedy, to the extent possible, the impact of the breach for those parties affected, including the possible notification of law enforcement officials, as appropriate.

If the breach involves an SSCP, then School must follow the procedure identified in section J of this policy.

All data security breaches must be recorded and reviewed for future prevention.

E. Use of and Disclosure to School Service Contract Providers

School may only disclose information to an SSCP for a legitimate educational purpose or with permission of the student's parent or student of majority age. School shall require, by contract, that each SSCP maintains a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student PII. The information security program must make use of appropriate administrative, technological, and physical safeguards. The SSCP must contractually agree to, following the termination or conclusion of the contract, destroy all student PII collected, generated, or inferred as a result of the contract.

School must ensure that the terms of any contract entered into with an SSCP on and after August 10, 2016 includes, at a minimum and in addition to other requirements found in this policy, the following requirements:

1. The SSCP must agree to comply with the requirements of this policy applicable to SSCPs, including use and destruction of data, and the ability for School to terminate the contract pursuant to section J of this policy.
2. The SSCP must agree to only collect, use, and share student PII as authorized by the contract or with the consent of the student who is the subject of the information, if student has reached majority age, or the student's parent;
3. The SSCP must agree to provide, and update as necessary, clear information that is understandable by a layperson explaining the data elements of student PII that the SSCP collects, the learning purpose for which the SSCP collects the student PII, and how the SSCP uses and shares the student PII. The information must include all student PII that the SSCP collects regardless of whether it is initially collected or ultimately held individually or in the aggregate. The SSCP must provide the information to School in a format that is easily accessible through a website, and School will post the information on its website, in accordance with this policy;
4. The SSCP must agree to provide clear notice to School before making material changes to its privacy policy for school services;
5. The SSCP must agree to facilitate any correction of factually inaccurate student PII at the request of School;
6. The SSCP must agree to immediately inform School upon its discovery of any misuse, data security breach, or unauthorized release of student PII held by the SSCP, a subcontractor of the SSCP, or a subsequent subcontractor of the SSCP,

regardless of whether the misuse, data security breach, or unauthorized release is a result of a material breach of the terms of the contract;

7. The SSCP must agree to not sell student PII; except in instances of purchase, merger, or other type of acquisition of a SSCP, or any assets of an SSCP, by another entity, and so long as the successor entity continues to be subject to the provisions of the contract with respect to student PII;
8. The SSCP must agree to not use or share student PII for purposes of targeted advertising to students;
9. The SSCP must agree to not use student PII to create a personal profile of a student other than as authorized by School for supporting the purposes of the contract or with the consent of the student, if student has reached the age of majority, or the student's parent;
10. Notwithstanding the other requirements of this policy, the SSCP contract will include a provision allowing the SSCP to use or disclose student PII to ensure legal or regulatory compliance or to take precautions against liability; to respond to or participate in the judicial process; to protect the safety of users or others on the school service contract provider's website, online service, online application, or mobile application; or to investigate a matter related to public safety, so long as the SSCP informs School of its use or disclosure as soon as possible.
11. The SSCP must agree to only share student PII with any subcontractor, or sub-subcontractor, that is providing a school service if the subcontractor, or sub-subcontractor, providing the school service is bound by the same requirements of this policy and the contract.

If an SSCP refuses to agree to those contractual requirements, School will not enter into a contract with that SSCP for school services, as that term is defined in this policy.

If it is determined by School that an SSCP, or a subcontractor or sub-subcontractor providing a school service, has committed a material breach of its contract that involves the misuse or unauthorized release of student PII, School Board of Director will determine whether to terminate the contract in accordance with section J of this policy.

School will post and regularly update on its website a list of the SSCPs with which School contracts, and a copy of each contract.

F. Use of and Disclosure to School Service On-demand Providers

School will, at the beginning and mid-point of each school year, request a list of the SSODPs being used by each staff person. School will, to the extent practicable, post to its website and regularly update a list of the SSODPs being used by School or its staff.

School will, at the request of a parent, assist in obtaining the data privacy policy of an SSODP being used by School or its staff.

School will post a notice on its website to SSODPs that explains the following:

> If School chooses to cease using the SSODP pursuant to this policy then School will post on its website the name of the SSODP, with any written response that the SSODP may submit, and that School will notify the Colorado Department of Education, which will also post on its website the SSODP's name and any written response.

If School has evidence that, in the estimation of School, demonstrates that an SSODP does not substantially comply with the SSODP's privacy policy or does not meet the requirements of this policy, School may choose to cease using the SSODP and prohibit employees from using the SSODP. If School chooses to cease using the SSODP it must notify the SSODP, and the SSODP will be asked to submit a written response.

School will post and regularly update on its website a list of any SSODPs that it chooses to cease using for the reasons described in this policy, and will include any written responses that it receives from the SSODP.

School will notify the Colorado Department of Education if it ceases using an SSODP for the reasons described in this policy and will provide a copy of any written response the SSODP.

G. Parent Notifications and Complaint Processes

School will make copies of this policy available upon request to the parent of a student and will post this policy on its website.

If a parent has a complaint, specific to the parent's child, regarding student data security and privacy the parent may submit a description of his or her complaint, including any relevant attachments or information to the Executive Director of School, who may attempt to remedy the parent's complaint. If the parent's complaint cannot be remedied, or if the parent desires to have his or her complaint heard by the Board of Directors, the Executive Director must forward the complaint to School Board of Directors and schedule a hearing within 45 days of receipt of the original complaint. At the hearing the Board of Directors will provide the parent an opportunity to be heard and may, in its discretion, ask questions of the parent or staff. The Board of Directors will render a decision or instruct the Executive Director on how to respond within 60 days of the date from which the Executive Director

received the complaint from the parent. Any decision made by the Board of Directors shall be final.

If a parent has evidence demonstrating that an SSODP being used by School or its employees does not substantially comply with the SSODP's privacy policy or does not meet the requirements specified in this policy, the parent may notify School and provide the evidence for consideration by School.

H. Staff Training

School will ensure that, at least annually, all staff who have access to student data, PII, or other sensitive information are trained to understand School policies and practices for proper collection, use, disclosure, maintenance, and destruction of student data, PII, or other sensitive information.

I. Data Security Audits

A regular and proactive audit policy helps to manage and reduce risks to School's information systems. Audits will be performed on a regular basis as required by law or executive management protocol.

The security auditor will be an external/independent third party (or at a minimum someone who is not operationally responsible for the area being audited), who evaluates systems for best practices and ensures compliance within an established set of requirements and controls.

The Executive Director will consider the following when determining the scope of the audit:

1. Security Vulnerabilities – Identify security vulnerabilities using reputable outside sources, and assign risk rankings (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

2. Risk Evaluation – Identify methods for evaluating vulnerabilities and assigning risk ratings to systems. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. Vulnerabilities are considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or result in a potential security compromise or breach if not addressed. Examples of critical educational systems include premise security, pupil accounting, learning management, general financial, and personnel systems. It also includes any public-facing system, database, or transmission mechanism around sensitive information or PII.

3. Automated Tools – Evaluates and recommends automated assessment tools and external resources that are suitable in identifying vulnerabilities including weak passwords, configuration issues, improper access controls, network penetration testing, and patch management issues.

4. Administrative Safeguards – Define protocols, policies, procedures, training plans and other administrative security controls useful to an auditor in comparing against a standard of operation.

5. Penetration Testing – Evaluate whether penetration testing may be used to identify system vulnerabilities. Examples of penetration testing include evaluations of firewalls and other external network entry points, analysis of software applications and websites, review of logging and account procedures, social engineering tests of staff.

Access to audit tools must be controlled and restricted to prevent possible misuse or compromise resources and log data. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to normal business operations.

Where possible, the Executive Director should use Certified Information Systems Auditors to audit the security controls of School systems.

The auditor's report will include the project scope, findings, and recommendations to enhance security. The Executive Director shall:

- Review the security auditor's report to confirm the findings and verify the security recommendations are sufficient and effective.

- Convey the findings to the appropriate personnel so that the findings and resolutions can be reviewed, understood, and remedied.

The Executive Director shall provide necessary reporting to the Board of Directors.

J. Enforcement

School must adequately train its employees and enforce its data privacy and security policies, procedures, processes, and practices to protect the privacy of every student and family from whom it collects data. School employees found to be in violation of this policy, in the sole discretion of School, may be subject to disciplinary action, up to and including termination.

In accordance with the SDTSA, any School Service Contract Provider, as that term is defined in the SDTSA, with a contract entered into after August 10, 2016 found to be in material breach of that contract or the requirements of the SDTSA involving the misuse or unauthorized release of student PII will be subject to having its contract with School terminated. School board, within a reasonable time after it is determined that a material breach occurred, shall hold a public hearing that includes discussion of the nature of the material breach, provides an opportunity for the contract provider to respond concerning the material breach, and any other public testimony, after which the board will render a decision to terminate or continue the contract.