Student Data Governance Policy

Contents

Introduction
- Purpose
- Scope and Applicability
- Non-Compliance
- Definitions
- Student Data Manager
- IT Systems Security Manager
- Technology Security Plan
- Public Posting of Policy and Procedure

Data Security
- Data Security
- Data Security & Privacy Training
- Data Breach
- Auditing and Review
- Employee Confidentiality Assurances

Data Disclosure
- Personally Identifiable Information (PII)
  - Student or Student's Parent/Guardian
  - School Officials
  - Directory Information
  - Third Party Vendors
  - Governmental Agency Requests
  - Internal Partner Requests
- Non-Personally Identifiable Student Data
- External Research or Evaluation

Record Retention and Expungement

FERPA Notice
- Annual FERPA Notice for Directory Information
- Parental Notification of Rights

Appendix
- Venture Academy Confidentiality Agreement
- Venture Academy Staff Acceptable Use Agreement
- Student Data Collection Notice

Introduction

Purpose

Venture Academy (the Academy) affirms that the efficient collection, analysis, and storage of student information are essential to maintain and improve the education of our students. The Academy recognizes the need to exercise care in the handling of confidential student information in all of its forms.

The Academy also acknowledges that the privacy of students and families and the use of the confidential information that we receive is protected by federal and state law (including the federal Family Educational Rights and Privacy Act (FERPA)), the Utah Family Educational Rights and Privacy Act, and the Utah Student Data Protection Act.

This Data Governance Policy (policy) is adopted pursuant to the Utah Student Data Protection Act and provides guidance regarding the collection, access, security, and use of educational data and how to protect student privacy while doing so. It is consistent with the Utah Student Data Protection Act regarding the access, security, and use of data maintained within the Academy. The Academy has established processes for the management of student data collection and use to comply with state and federal law.

Scope and Applicability

This policy is designed to ensure only authorized disclosure of confidential information and is applicable to all paid employees of the Academy, its Board of Directors, volunteers who have access to student data, and contractors of the Academy. The policy governs all access agreements made to disclose data to third parties. It must be used to assess the risk of any given disclosure. The policy will be reviewed regularly and, if needed, amended.

Non-Compliance

Non-compliance with the requirements of this policy may result in loss of access to student data and the networks on which it is maintained. Employees, board members, and contractors may be subject to disciplinary action up to and including termination of employment, termination of board membership, and termination of any agreement under which contract work is performed.

Definitions

Administrative Security System consists of policies, procedures, trainings, personnel controls (including security policies), audits, supervision, hiring procedures, user control access, background checks, performance evaluations, disaster recovery, breach protocols, contingency plans, and emergency plans. These measures ensure that authorized users know and understand how to properly use the policy and system in order to maintain security of data.

Aggregate Data is collected or reported about a group, cohort, or institutional level and does not contain Personally Identifiable Information (PII).

Data Breach is the unauthorized release or acquisition of a student's PII.

Technical Security describes the hardware and software-based safeguards the Academy employees, including user identification and password access, authenticating, access rights, and authority levels. These measures ensure that only authorized users are able to perform functions or actions they are authorized to do.

Physical Security describes security measures designed to deny unauthorized access to facilities or equipment.

Personally Identifiable Information (PII) includes: protected information that is linked or linkable to any part of the student's name, nickname, or preferred name, the name of the student's family, the student's address, the student's social security number, any unique identification number or biometric record associated with the student, or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name. Additionally, this may includes medical information, court orders and/or any other legal documentation, behavioral and disciplinary records, I.E.P. information, 504 plan information, immunization records, and assessment/academic record data. This also includes other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school's community who does not have personal knowledge of the relevant circumstances to identify the student (this includes potential PII that results from too low of n-size).

Student Data means data collected at the student level and included in a student's educational records. Student data may or may not be PII, but does not include aggregate data.

Unauthorized Data Disclosure is the intentional or unintentional release of PII to an unauthorized person, organization, or environment.

Student Data Manager

The Student Data Manager has the following duties:

- Authorize and manage the sharing--outside of the Academy--of PII from any record of the Academy;
- Act as the primary local point of contact for the State of Utah's student data officer.
- Oversee the Academy's compliance with applicable laws governing the use and sharing of PII;
- Create and maintain a list of all Academy staff, board members, and volunteers that have access to PII.;
- Ensure annual training on data privacy to all staff members, board members, and volunteers. Document all staff names, training dates, and times of training.

The Student Data Manager for the Academy is the District Secretary.

IT Systems Security Manager

The IT Systems Security Manager oversees the technical security aspects of our Data Privacy plan, regularly updates technological security protocols and systems, and advises administration when security upgrades are recommended or needed. At the direction of administration, the IT Systems Security Manager may help investigate if there is a technology-based data breach.

Technology Security Plan

The Academy will develop and maintain a Technology Security Plan which complies with all federal and state privacy and data governance laws. Including the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

Public Posting of Policy and Procedure

The Academy will post this policy on its website along with its associated Metadata Dictionary.

Data Security

Data Security

The Academy has Administrative Security, Physical Security, and Technical Security controls to protect against a data breach or an unauthorized data disclosure.

Data Security and Privacy Training

The Academy will provide an annual training prior to the first day of school for all employees and volunteers who have access to student data. The Board of Directors will receive annual training during their August board meeting. This training will provide education on data security and minimize the risk of human error and misuse of information. Additionally:

- All Academy board members, employees, and volunteers with access to student data must sign and follow the Venture Academy Employee Acceptable Use Policy (See example, Appendix B), which describes permissible uses of Academy technology and information;
- Contractors will annually sign and acknowledge they have read and understand this plan and will implement any additional direction concerning data security given to them by the Student Data Manager and/or Administration. All contractors must also be compliant with Utah's Student Data Protection Act;
- Participation in the training will be annually monitored by Administration and the Student Data Manager. Any absences will be reported to Administration and a make-up session will be scheduled accordingly.

Data Breach

In the event of a data breach or other inadvertent release of PII, the Academy will follow industry best practices for responding to the breach. Additionally, the Academy will comply with all notification requirements imposed by law, including parent/legal guardian notification of any student data breaches.

Concerns about data breaches should be reported to the Student Data Manager who will collaborate with Administration to determine if/when the reported data breach occurred. The Administration will then identify appropriate actions and/or consequences.

Auditing and Review

The Student Data Manager will conduct an annual review of existing data access, policy, and security safeguards. Any changes to data access, the policy, or security will be collaboratively built with Administration.

Employee Confidentiality Assurances

The Venture Academy Confidentiality Agreement is signed during the first week of employment/service (See example, Appendix A).

Data Disclosure

Personally Identifiable Information

Student or Student's Parent/Guardian

A student owns their PII. The Academy will provide parents or legal guardians with access to their child's student data as soon as possible, but at least within 45 days of receiving an official request in writing that is submitted to an Administrator.

The Academy is not required to provide data that it does not maintain, nor is the Academy required to create Student Data in response to an eligible student's request.

School Officials

School officials may have access to PII if the school official is determined to have a legitimate educational interest in that information. Examples of school officials are, but are not limited to: administrators, teachers, secretaries, school counselors, deans, and paraeducators.

Directory Information

The Academy can disclose directory information as defined and allowed under the federal FERPA and the Utah Family Educational Rights and Privacy Act.

Third Party Vendors

Third party vendors may have access to student's PII if the vendor is designated by the Academy as a "school official" as defined in FERPA. A school official may include vendors such as: nurses, counselors, attorneys, probation officers, consultants, or other parties to whom the school has outsourced institutional services or functions.

All third party vendors contracting with the Academy must be compliant with Utah's Student Data Protection Act.

Governmental Agency Requests

The Student Data Manager or Administration can disclose PII under the following circumstances:

- To an authorized caseworker or other representative of the Department of Human Resources or the Juvenile Court or a law enforcement officer that is acting in their official duty;
- In response to a lawfully issued subpoena and/or court order, after complying with applicable requirements under FERPA;
- As otherwise allowed by law, such as with a valid parent/guardian consent.

In the case of a federal or state government agency request for PII, the requesting agency must provide evidence of the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent, such as:

- Reporting requirement;
- Audit;
- Evaluation.

The student data manager will ensure the proper data disclosure protections are included if necessary. An Interagency Agreement must be reviewed and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

Internal Partner Requests

Internal partners to the Academy include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented by the Student Data Manager.

Non-Personally Identifiable Student Data

External data requests from individuals or organizations that do not intend to conduct external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation should be made to the Student Data Manager. The requests will be reviewed with Administration. The Academy reserves the right to grant or deny requests based on the best interests of the Academy and its membership.

Record Retention and Expungement

Venture Academy recognizes the risk associated with data following a student year after year that could be used to mistreat the student. Venture Academy shall review all requests for records expungement from parents and make a determination based on the following procedure.

Procedure

The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.

1. If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
2. Venture Academy shall decide whether to expunge the data within a reasonable time after the request.
3. If Venture Academy decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
4. Venture Academy shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. Venture Academy shall provide the parent notice of the date, time, and place in advance of the hearing.
6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
7. Venture Academy shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
8. Venture Academy shall make its decision in writing within a reasonable time following the hearing.
9. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.

10. If the decision is to expunge the record, Venture Academy will seal it or make it otherwise unavailable to other staff and educators.

FERPA Notice

Family Educational Rights and Privacy Act (FERPA) Notice for Directory Information

The Family Educational Rights and Privacy Act (FERPA), a Federal law, requires that Venture Academy, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, Venture Academy may disclose appropriately designated "directory information" without written consent, unless you have advised Venture Academy to the contrary in accordance with procedures. The primary purpose of directory information is to allow Venture Academy to include this type of information from your child's education records in certain school publications. Examples include:

• A playbill, showing your student's role in a drama production;
• The annual yearbook;
• Honor roll or other recognition lists;
• Graduation programs;

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters and institutions of higher education, upon request, with directory information unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.[1]

If you do not want Venture Academy to disclose directory information from your child's education records without your prior written consent, you must notify Venture Academy in writing by the first day of school or by the first day of attendance. Venture Academy has designated the following information as directory information:

- Student name
- Parent name

[1] These laws are: Section 9528 of the Elementary and Secondary Education Act (20 U.S.C. § 7908) and 10 U.S.C. § 503(c). ADA Compliant 02/26/2018

- Photographs, to be used on websites, publications, or similar promotional/celebratory reasons.
- Grade level
- Participation in officially recognized activities and sports
- Degrees, honors, and awards received

Notification of Rights under FERPA

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the Venture Academy receives a request for access. Parents or eligible students who wish to inspect their child's or their education records should submit to the student data manager or school principal a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Parents or eligible students who wish to ask Venture Academy to amend their child's or their education record should write the student data manager or school principal, clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent. One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. The criteria for determining who constitutes a school official and what constitutes a legitimate educational interest must be set forth in the school's or school district's annual notification for FERPA rights. Upon request, the school discloses education records without consent to officials of another school or school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer.

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the Venture Academy to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202

FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in § 99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, § 99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student –

- To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in § 99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(3) are met. (§ 99.31(a)(1))

- To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of § 99.34. (§ 99.31(a)(2))

- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the State educational agency (SEA) in the parent or eligible student's State. Disclosures under this provision may be made, subject to the requirements of § 99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf, if applicable requirements are met. (§§ 99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary for such purposes as to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§ 99.31(a)(4))

- To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to § 99.38. (§ 99.31(a)(5))

- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction, if applicable requirements are met. (§ 99.31(a)(6))

- To accrediting organizations to carry out their accrediting functions. (§ 99.31(a)(7))

- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§ 99.31(a)(8))

- To comply with a judicial order or lawfully issued subpoena if applicable requirements are met. (§ 99.31(a)(9))

- To appropriate officials in connection with a health or safety emergency, subject to § 99.36. (§ 99.31(a)(10)

- Information the school has designated as "directory information" if applicable requirements under § 99.37 are met. (§ 99.31(a)(11))

- To an agency caseworker or other representative of a State or local child welfare agency or tribal organization who is authorized to access a student's case plan when such agency or organization is legally responsible, in accordance with State or tribal law, for the care and protection of the student in foster care placement. (20 U.S.C. § 1232g(b)(1)(L))

- To the Secretary of Agriculture or authorized representatives of the Food and Nutrition Service for purposes of conducting program monitoring, evaluations, and performance measurements of programs authorized under the Richard B. Russell National School Lunch Act or the Child Nutrition Act of 1966, under certain conditions. (20 U.S.C. § 1232g(b)(1)(K))

Appendix

Appendix A

Venture Academy Confidentiality Agreement

Discretion and confidentiality are of utmost importance and a requirement for working or volunteering at Venture Academy Charter School.

The following are guidelines for maintaining ethical standards concerning privacy:
- Respect the dignity, privacy, and individuality of all students, families, and staff at all times.
- Refer concerns about privacy to an administrator.
- Student's progress or any information pertinent to a student or student(s) shall only be shared with parents/guardians who have legal release to that information or to school officials as directed by the Student Data Manager or an administrator.
- Confidential information regarding disability, performance, or personal circumstances shall only be shared with school officials in the appropriate setting.

I, _____, have read, understand, and agree to abide by the above ethical standards. I understand that it is possible that by disclosing information of a confidential nature my employment/volunteer status may be terminated.

I am a(n) (mark one):

o Employee
o Substitute
o Volunteer with access to Personally Identifiable Information
o Board Member
o Third Party Contractor

_____ _____
Signature Date

Appendix B

Venture Academy Staff Acceptable Use Agreement

Introduction:
Venture Academy recognizes the need for a policy governing the use of the electronic information resources by board members, employees, volunteers with access to PII data, and contractors. Staff as outlined in Utah State Code Â§53A-3-422. Responsibility is delegated to the Administration for implementing the policy according to established guidelines.
Electronic information resources will be available to qualifying students at Venture Academy. These resources include access to the Internet and other network files or accounts. Our goal in providing electronic services is to promote educational excellence by facilitating resource sharing, innovation, and communication.

Administration Policy:
Student use of electronic information resources must be in support of education and research and must be consistent with the educational objectives of Venture Academy. While access to all materials on a worldwide network cannot be controlled, Internet access at Venture Academy is filtered and monitored on an ongoing basis.
Internet resources can be valuable for a student's education. School internet access is a privilege which may be authorized as well as withdrawn. Staff members are expected to be aware of and abide by the following:

1. Personal Safety and Privacy
Personal contact information is to be shared with caution. Entering or otherwise disclosing personal information of others is strictly prohibited beyond normal registry type information.

2. Internet Use
Board members, employees, volunteers, and contractors may use school Internet access for educational purposes. If any of the above groups formally publish school related information on the Internet they must have approval from the Director to do so.

3. Board Members, employees, volunteers, and contractors are strictly prohibited from:

- Accessing or creating offensive, profane, or pornographic files.
- Use Internet games, MUDs (Multi-user domains), MMOs (Massively Multiplayer Online games) or web chats.
- Plagiarizing works or violating copyrights or trademarks
- Attempt to bypass computer security

4. Expectation of Privacy

Any user of Venture Academy's networks, software, hardware, or internet access do not have an expectation of privacy in files, disks, documents, Internet history, etc., which have been used or created with Venture Academy equipment.

5. Vandalism
Vandalism is defined as any malicious attempt to harm or destroy property of the user, another user or of any other agencies or networks that are connected to the Network or the Internet system. Vandalism also includes, but is not limited to: abusive overloading of data on the server or the uploading, downloading or creation of computer viruses. Any engagement in network vandalism constitutes unacceptable use and will subject the student to appropriate disciplinary action.

6. Security
Security on any computer system is a high priority because of multiple users. Do not use another individual's account or any other login other than your own at any time. Any security concern must be reported to the principal, teacher/supervisor or systems administrator.

7. Disciplinary Actions
The use of electronic information resources is a privilege, not a right. Inappropriate use of these resources may result in disciplinary action up to and including termination of employment. Actions may be referred to legal authorities. The administration, teacher/supervisor or systems administrator may limit, suspend or revoke access to electronic resources at any time.

Signature of Agreement:

Rules of conduct are described in this "Acceptable Use Agreement" for Venture Academy and apply when the electronic information system is in use. I understand any violations of the above provisions will result in the loss of my user account and may result in further disciplinary and/or legal action. I therefore agree to maintain acceptable standards and to report any misuse of the system to the Director.

Name (Please Print): _____

Position: _____

Staff Signature: _____

Date: _____

Appendix C

Student Data Collection Notice

Necessary Student Data

Necessary student data means data required by state statute or federal law to conduct the regular activities of the school:

- Student Name, Date of birth, and Sex
- Parent and student contact information and Custodial parent information
- A student identification number
- Local, state, and national assessment results or an exception from taking a local, state, or national assessment
- Courses taken and completed, credits earned, and other transcript information
- Course grades and grade point average
- Grade level and expected graduation date or graduation cohort
- Degree, diploma, credential attainment, and other school information
- Attendance and mobility
- Drop-out data
- Immunization record or an exception from an immunization record
- Race, Ethnicity, or Tribal affiliation
- Remediation efforts
- An exception from a vision screening required under Section 53G-9-404 or information collected from a vision screening described in Utah Code Section 53G-9-404
- Information related to the Utah Registry of Autism and Developmental Disabilities (URADD), described in Utah Code Section 26-7-4
- Student injury information
- A disciplinary record created and maintained as described in Utah Code Section 53E-9-306
- Juvenile delinquency records
- English language learner status
- Child find and special education evaluation data related to initiation of an IEP

Optional Student Data

We may only collect optional student data with written consent from the student's parent or from a student who has turned 18:

- Information related to an IEP or needed to provide special needs services
- Biometric information used to identify the student
- Information required for a student to participate in an optional federal or state program (e.g., information related to applying for free or reduced lunch)

Certain sensitive information on students collected via a psychological or psychiatric examination, test, or treatment, or any survey, analysis, or evaluation will only be collected with parental consent. You will receive a separate consent form in these cases.

Prohibited Collections

We will not collect a student's social security number or criminal record, except as required by Utah Code Section 78A-6-112(3).

Data Sharing

We will only share student data in accordance with the Family Educational Rights and Privacy Act (FERPA), which generally requires written parental consent before sharing student data. FERPA includes several exceptions to this rule, where we may share student data without parental consent. For more information on third parties receiving student information from us, see our Metadata Dictionary.

Student data will be shared with the Utah State Board of Education via the Utah Transcript and Records Exchange (UTREx).

Benefits, Risks, and Parent Choices

The collection, use, and sharing of student data has both benefits and risks. Parents and students should learn about these benefits and risks and make choices regarding student data accordingly. Parents are given the following choices regarding student data:

- Choice to request to review education records of their children and request an explanation or interpretation of the records (see our annual FERPA notice for more information)
- Choice to contest the accuracy of certain records (see our annual FERPA notice for more information), potentially leading to the correction, expungement, or deletion of the record
- Choice to opt into certain data collections (see the section above on optional data collections)
- Choice to opt out of certain data exchanges:
    - Information that has been classified as directory information (see our directory information notice for more information)
    - Parents of students with an IEP may have their information shared with the Utah Registry of Autism and Developmental Disabilities (URADD). If included in this data exchange, parents will receive a separate notice within 30 days of the

exchange, informing them of their right to opt out, per Utah Code Section 53E-9-308(6)(b)

- Choice to file a complaint if you believe the school or its agents are violating your rights under FERPA or Utah's Student Data Protection Act. If you have a complaint or concern, we recommend starting locally and then escalating to the state and US Department of Education

Storage and Security

In accordance with Board Rule R277-487-3(14), we have adopted a cybersecurity framework.