Career Academy of Utah Data Governance Plan

Career Academy of Utah has a contractual relationship established with Stride-K12, as its ESP (Education Services Provider), including ESP-provided IT/technology platforms and associated security, applications and services, the ESP, and the LEA (Local Education Agency) Board follow NIST CSF (National Institutes of Standards & Technology Cybersecurity Framework) guidelines to ensure industry standard practices for potential cyber security risks and to protect information and data.

ESP-provided IT/technology platforms, including endpoints, are monitored by the Stride-K12 IT Technology team 24/7.

1. Governing Principles

Career Academy of Utah (referred to as the school or CAU throughout) takes its responsibility toward student data seriously. This governance plan incorporates the following Generally Accepted Information Principles (GAIP):

- **Risk:** There is risk associated with data and content. The risk must be formally recognized, either as a liability or through incurring costs to manage and reduce the inherent risk.
- **Due Diligence:** If a risk is known, it must be reported. If a risk is possible, it must be confirmed.
- **Audit:** The accuracy of data and content is subject to periodic audit by an independent body.
- **Accountability:** An organization must identify parties which are ultimately responsible for data and content assets.
- **Liability:** The risk in information means there is a financial liability inherent in all data or content that is based on regulatory and ethical misuse or mismanagement.

2. Data Maintenance and Protection Policy

CAU recognizes that there is risk and liability in maintaining student data and other education-related data and will incorporate reasonable data industry best practices to mitigate this risk.

2.1 Process

In accordance with R277-487, CAU shall do the following:

- Designate a Data Manager and Information Security Officer.
- Maintain and protect student CUM files, staff files and other educational documents containing personal identifiable in a secure location with limited access.
- Use applicable NIST CSF guidelines as an equivalent to CIS controls to ensure the protection of student data.
- Annually complete USBE's Cybersecurity Framework Survey.

3. Roles and Responsibilities Policy

CAU acknowledges the need to identify parties who are ultimately responsible and accountable for data and content assets. These individuals and their responsibilities are as follows:

3.1 Data Manager roles and responsibilities

- Provide necessary technical assistance, training, and support.
- Develop processes and procedures that adhere to the contents of the data governance plan.
- Maintain the school metadata dictionary.
- Act as the primary local point of contact for the state student data officer.
- Ensure that the following notices are available to parents and posted on the school website.
    - annual FERPA notice
    - directory information policy
    - survey policy and notice
    - data collection notice
- Authorize and manage the sharing, outside of the student data manager's education entity, of personally identifiable student data for the education entity as described in this section.
    - The sharing of student personally identifiable data from a cumulative record outside of the school will not be released without parent permission.
    - The school may share the personally identifiable student data of a student with the student and the student's parent if the student is under 18 years of age.

3.2 Information Security Officer

- Collaborate with the ESP IT/Technology group to ensure applicable use of NIST CSF guidelines as an equivalent to CIS controls to ensure the protection of student data.
- Provide and/or coordinate necessary technical assistance, training, and support as it relates to IT security.

4. Training and Support Policy

CAU recognizes that training and supporting educators and staff regarding federal and state data privacy laws is a necessary control to ensure legal and regulatory compliance.

4.1 Procedure

1. The data manager will ensure that educators who have access to student records will receive an annual training on confidentiality of student data and student privacy laws.
2. The data manager will maintain a tracking record of completed training for all CAU employees.
3. By October 1 each year, the data manager will report to USBE the completion status of the annual confidentiality training and provide a copy of the training materials used.
4. The data manager shall keep a list of all employees who are authorized to access student education records after the required training is completed.

5. Audit Policy

In accordance with the risk management priorities of CAU, CAU and ESP's (Stride-K12) compliancy team will conduct an audit of this governance plan on an annual basis.

6. Data Sharing Policy

There is a risk of redisclosure whenever student data is shared. CAU shall follow appropriate controls to mitigate the risk of redisclosure and to ensure compliance with federal and state law.

6.1 Procedure

1. The data manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA. CAU may share a student's personally identifiable student data from a cumulative record with:

    a. a school official
    b. school staff with a legitimate educational purpose and consistent with their educator obligations
    c. legal officials in response to a subpoena issued by a court
    d. an authorized caseworker or other representative of the Utah Department of Human Services if:
    e. (a) the Department of Human Services is:
        i. (i) legally responsible for the care and protection of the student; or
        ii. (ii) providing services to the student;
    f. (b) the student's personally identifiable student data is not shared with a person who is not authorized:
        i. (i) to address the student's education needs; or
        ii. (ii) by the Department of Human Services to receive the student's personally identifiable student data; and
    g. (c) the Department of Human Services maintains and protects the student's personally identifiable student data, or a person to whom CAU has outsourced a service or function:
        i. (i) that the education entity's employees would typically perform; or
        ii. (ii) to research the effectiveness of a program's implementation.

2. For external research, the data manager shall ensure that the study follows the requirements of FERPA's study exception.
    a. CAU may share aggregate data upon request, with the elimination of personally identifiable student data, for external research or evaluation.
3. After sharing student records, the data manager shall ensure that an entry is made in the school Metadata Dictionary to record that the exchange happened.
4. After sharing from student records, the data manager shall make a note in the student record of the exchange.

7. Expungement Request Policy

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

7.1 Procedure

To ensure maximum student data privacy, CAU will delete student data once administrative need has ended and in accordance with the active records retention schedule timeline.

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

The procedure for expungement is as follows

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. CAU shall decide whether to expunge the data within a reasonable time after the request.
3. If CAU decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
4. CAU shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. CAU 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. CAU 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. CAU 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, CAU will seal it or make it otherwise unavailable to other staff and educators.

8. Data Breach Response Policy

CAU shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, CAU staff shall follow industry best practices for responding to the breach, and as described below.

Within the contractual relationship established with Stride-K12, as its ESP (Education Services Provider), including ESP-provided IT/technology platforms and associated security, applications and services, the ESP and the LEA (Local Education Agency) Board follow NIST CSF (National Institutes of Standards & Technology Cybersecurity Framework) guidelines to ensure industry standard practices for potential cyber security risks and to protect information and data.

ESP-provided IT/technology platforms, including endpoints, are monitored by the Stride-K12 IT Technology team 24/7.

The School Cyber Incident Response Team (SCIRT) includes:

- LEA Head of School/Executive Director
- LEA/School Information Security Officer
- ESP Portfolio Vice President assigned to the School
- ESP IT / Technology Team, including Information Security (InfoSec)

Detection: Potential risks can be detected at:

- the ESP IT/Technology platform level by utilizing Endpoint Detection Response (EDR) and enterprise security monitoring tools and existing End user reporting methods
- and/or at
- the LEA/School level via verbal or other electronic communication from/to Parents/Students/Families via their Teachers, other Instructional Staff, or Administrative Staff.

In either case process will include the LEA Head of School/Executive Director and LEA/School Information Security Officer notifying or being notified by the ESP IT Technology/InfoSec team (in collaboration with ESP Portfolio Executive assigned to the School) to ensure proper due diligence and management to collect, analyze, determine root cause, remediate, communicate, respond, and report information on real or perceived security incidents both internal and external, and bring to conclusion.

In the event of a Significant Data Breach as described in Note 1 below, the LEA Head of School/Executive Director and LEA/School Information Security Officer, in collaboration with the ESP School Portfolio Vice President and ESP IT / Technology team, will communicate to an LEA Board designee and the Board, including coordination with legal counsel. and determine which entities and individuals need to be notified.

Note: This policy is subject to amendment in accordance with guidance from the Utah State Board of Education (USBE) following the enactment of recently passed privacy laws.

8.1 Notification

CAU shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

CAU shall always notify:

- The parent or the adult student in the case of a significant data breach
- USBE of any data breach from a third party.

9. Publication Policy

CAU recognizes the importance of transparency and will post this policy on the school website.