The Center for Creativity, Innovation and Discovery

Student Data Privacy and Security

Statement of Disclosure

The Center for Creativity, Innovation and Discovery ("CCID") affirms that the efficient collection, analysis, and storage of student information are essential to improve the education of our students. CCID recognizes the need to exercise care in the handling of confidential student information as the use of student data has increased and as technology has advanced. CCID also acknowledges that the privacy of students and the use of confidential student information is protected by federal and state laws, including the Family Educational Rights and Privacy Act (FERPA) and the Utah Student Data Protection Act of 2016.

CCID's *Student Data Privacy and Security Policy* is intended to provide disclosure and guidance regarding the collection, access, security and use of education data to protect student privacy. It is consistent with the Utah Student Data Protection Act regarding the access, security, and use of data maintained within the school. CCID has established processes for managing student data collection and use to comply with state law. The school has also designated the Executive Director as CCID's Student Data Privacy Manager. CCID acknowledges that violation of the Utah Student Data Protection Act may result in civil penalties.

Defined Terms

Administrative Security consists of policies, procedures, and personnel controls including security policies, training, audits, technical training, supervision, separation of duties, rotation of duties, recruiting and termination procedures, user access control, background checks, performance evaluations, disaster recovery, contingency, and emergency plans. These measures ensure that authorized users know and understand how to properly use the system in order to maintain security of data.

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

Data Breach is the unauthorized acquisition of PII.

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authenticating, access rights, and

authority levels. These measures ensure that only authorized users are able to perform actions or access information in a network or a workstation.

Personally Identifiable Information (PII) includes: a student's name; the name of the student's family; the student's address; the student's social security number; a student education unique identification number or biometric record; or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name; and other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances to identify the student.

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

Student Data means data collected at the student level and included in a student's educational records.

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

Collection

CCID follows applicable state and federal laws related to student privacy in the collection of student data.

Access

- Unless prohibited by law or court order, CCID provides parents, legal guardians, or eligible students, as applicable, the ability to review their child's educational records and student performance data as per state and federal law;
- CCID allows for authorized purposes, uses, and disclosures of data maintained by CCID as a Local Education Agency (LEA);
- The Executive Director is responsible for granting, removing, and reviewing user access to student data.
- CCID allows parents, students, and the public access to information about student data privacy and the security safeguards that protect the data from unauthorized access and use;
- CCID provides contact information and a process for parents and students to request student and public school information from CCID consistent with the law;
- CCID's Audit Committee conducts an annual review of existing access and security safeguards;

- Access to PII maintained by CCID shall be restricted to: (1) the authorized staff of CCID who require access to perform their assigned duties; and (2) authorized employees of the Utah State Board of Education who require access to perform their assigned duties; and (3) vendors who require access to perform their assigned duties.
- CCID's Student Data Privacy Manager may not share PII outside of the school as an education entity without a data authorization except:
    - With the student and the student's parent;
    - With a school official;
    - With an authorized caseworker or other representative of the Department of Human Services or Utah Juvenile Court, Division of Juvenile Justice Services, Division of Child and Family Services, Division of Services for People with Disabilities;
    - In response to a subpoena issued by a court, but not outside of the use described in the subpoena; and
    - With a person to whom the Student Data Privacy Manager's education entity has outsourced a service or function to research the effectiveness of a program's implementation or to perform a function that the education entity's employees would typically perform.
- The Student Data Privacy Manager may not share PII for the purpose of external research or evaluation.

Security

- CCID has in place administrative security, physical security, and logical security controls to protect from a data breach or an unauthorized data disclosure.
- CCID shall immediately notify the State Charter Director and the State Superintendent of Public Instruction in the case of a confirmed data breach or a confirmed unauthorized data disclosure.
- CCID shall also notify in a timely manner affected individuals, students, and families if there is a confirmed data breach or a confirmed unauthorized data disclosure.
- If there is a release of a student's PII due to a security breach, CCID shall notify the student, if the student is an adult student. If the student is not an adult student, CCID will notify the student's parent or legal guardian.
- In accordance with R277-487-6, CCID acknowledges that data maintained by CCID, including data provided by contractors, may not be sold or used for marketing purposes (except with regard to authorized uses or directory information not obtained through a contract with an educational agency or institution).

Using and Expungement of Data

- At the end of a three year period adult students, or parents of a student may request in writing that the following student data may be expunged:
    - Medical records; and
    - Behaviorial test assessments
- The following types of student data that may not be expunged, includes:
    - Grades
    - Transcripts
    - A recorder of the student's enrollment
    - Assessment information
- CCID may create and maintain a cumulative disciplinary record for a student
    - CCID may expunge a student's student data that is stored by the education entitiy if:
        - The student is at least 23 years old; and
        - The student requests that the education entity expunges the student data.
- CCID shall retain and dispose of records in accordance with Section 63G-2-604.

Disclosure Statement

- Publicly released reports shall not include PII and shall use aggregate data in such a manner that re-identification of individual students is not possible.
- CCID has clearly defined in its communication policy and in registration materials for parents what data is determined to be directory information.
- CCID notifies parents in writing at registration about directory information which includes PII and offers parents an opportunity to opt out of the directory. If a parent does not opt out, the release of the information as part of the directory is not a data breach or an unauthorized data disclosure.
- CCID provides a disclosure statement to parents or guardians of CCID students that meets the following criteria:
    - A prominent, stand-alone document;
    - Annually updated and published on CCID's website;
    - States the necessary and optional student data that CCID collects;
    - States that CCID will not collect student data prohibited by the Utah Student Data Protection Act;
    - States that CCID will not share legally collectible data without authorization;

- States that students and parents are responsible for the collection, use, or sharing of student data as described in Section 53A-1-1405 which states that a student owns his/her personally identifiable student data and that a student may download, export, transfer, save, or maintain the student's data, including documents;
- Describes how CCID may collect, use, and share student data;
- Includes the following statements: "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."
- Describes in general terms how CCID stores and protects student data; and
- States a student's rights related to his/her data.

- CCID trains employees, aides, and volunteers regarding confidentiality of personally identifiable student information and student performance data, as defined in FERPA.

Third Party Vendors

- CCID's contracts with outside vendors involving student data, which govern databases, online services, assessments, special education or instructional supports, shall include the following provisions which are intended to safeguard student privacy and the security of the data:
  - Requirement that the third party provider meet the definition of a school official under 34 CFR 99.31 (a)(1)(i)(B);
  - Requirement that the contract between the LEA and the third party provider include a provision that the data is the property of CCID;
  - Requirement that the vendor agree to comply with all applicable state and federal law;
  - Requirement that the vendor have in place administrative security, physical security, and logical security controls to protect from a data breach or unauthorized data disclosure;
  - Requirement that the vendor restrict access to PII to the authorized staff or the vendor who require such access to perform their assigned duties;
  - Prohibition against the vendor's secondary use of PII including sales, marketing or advertising;
  - Requirement that CCID monitor and maintain control of the data;
  - Requirement that, if CCID contract with a third party provider to collect and have access to CCID's data as described in R277-487-3B(5), CCID notify

a student and the student's parent or guardian in writing that the student's data is collected and maintained by the third party provider;
    - Requirement for data destruction and an associated timeframe; and
    - Penalties for non-compliance with the above provisions.

- CCID's Third Party Contractors are legally allowed to engage in the following activities:
    - The use of student data for adaptive learning or customized student learning purposes;
    - Market an educational application or product to a parent or legal guardian of a student if the third party contractor did not use student data, shared by or collected on behalf of CCID, to market the educational application or product;
    - Use a recommendation engine to recommend to a student services or content that relates to learning or employment within the third party contractor's internal application, if the recommendation is not motivated by payment or other consideration from another party;
    - Respond to a student request for information or feedback, if the content of the response is not motivated by payment or other consideration from another party;
    - Use student data to allow or improve the operability and functionality of the third party contractor's internal application.

- At the completion of a contract with CCID, if the contract has not been renewed, a third party contractor shall return all personally identifiable student data to CCID, and as reasonably, delete all personally identifiable student data related to the third party contractors work.

- A third party contractor may not (except as provided in Subsection 6(b) of the Utah Student Data Protection Act):
    - Sell student data;
    - Collect, use, or share student data, if the collection, use, or sharing of the student data is inconsistent with the third party contractor's contract with CCID; or
    - Use student data for targeted advertising.

- A person may obtain student data through the purchase of, merger with, or otherwise acquiring a third party contractor if the third party contractor remains in

compliance with state and federal law, this policy, and CCID's previous contract with the original third party.

- The provisions of this section of CCID's *Student Data Privacy and Security Policy* do not apply to the use of an external application, including the access of an external application with login credentials created by a third party contractor's internal application; nor do they apply to the providing of Internet service; nor do they impose a duty on a provider of an interactive computer service, as defined by the Utah Student Data Protection Act.