Canyon Rim Academy Data Governance Plan
October 26, 2017 recodified 9-11-2019

1 PURPOSE

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data; from acquisition, to use, to disposal. The Utah State Board of Education and Canyon Rim Academy (CRA) take seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-303 requires that CRA adopt a Data Governance Plan.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, and contractors of CRA. The policy must be used to assess agreements made to disclose data to third-parties. This policy must also be used to assess the risk of conducting business. In accordance with CRA policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information. The following 7 subsections provide data governance policies and processes for CRA:

1. Non-Disclosure Assurances for Employees
2. Data Security and Privacy Training for Employees
3. Data Disclosure
4. Data Breach
5. Record Retention and Expungement
6. Data Quality
7. Transparency

Furthermore, this CRA Data Governance Plan works in conjunction with the CRA Technology Security Policy, which:

- Designates the principal and the principals' secretary as the stewards for all confidential information maintained within CRA.
- Designates Data Stewards access for all confidential information.
- Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
- Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards and plans.
- Complies with all legal, regulatory, and contractual obligations regarding privacy of Agency data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting CRA standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all CRA board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
- Provides policies and process for

- Systems administration,
- Network security,
- Application security,
- Endpoint, server, and device Security
- Identity, authentication, and access management,
- Data protection and cryptography
- Monitoring, vulnerability, and patch management
- High availability, disaster recovery, and physical protection
- Incident Responses
- Acquisition and asset management, and
- Policy, audit, e-discovery, and training.

The following table outlines individual CRA staff responsibilities.

Role	Responsibilities
Student Data Manager	1. authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity 2. act as the primary local point of contact for the state student data officer. 3. A student data manager may share personally identifiable student data that are: a. of a student, with the student, and the student's parent b. required by state or federal law c. in an aggregate form with appropriate data redaction techniques applied d. for a school official e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court f. in response to a subpoena issued by a court. g. directory information h. submitted data requests from external researchers or evaluators, 4. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation. 5. Create and maintain a list of all LEA staff that has access to personally identifiable student data. 6. Ensure annual LEA level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas.
IT Systems Security Manager	1. acts as the primary point of contact for state student data security administration in assisting the board to administer this part; 2. ensures compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable CRA employees; and b. producing resource materials, model plans, and model forms for LEA systems security; 3. investigates complaints of alleged violations of systems breaches; 4. provides an annual report to the board on CRA's systems security needs
Educators	1. Receive annual training and sign off on the Employee Non-Disclosure Agreement.

3 EMPLOYEE NON-DISCLOSURE ASSURANCES

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

3.1 SCOPE

All CRA board members, employees, contractors and volunteers must sign and obey the CRA Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information.

3.2 NON-COMPLIANCE

Non-compliance with the agreements shall result in consequences up to and including removal of access to CRA network; if this access is required for employment, employees and contractors may be subject to dismissal.

3.3 NON-DISCLOSURE ASSURANCES

All student data utilized by CRA is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way CRA staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all CRA staff to verify agreement to adhere to/abide by these practices and will be maintained in CRA Human Resources. All CRA employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the Chief Privacy Officer.
3. Consult with CRA internal data owners when creating or disseminating reports containing data.
4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on appropriate-secured location. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at CRA when disposing of such records.
9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).

11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager should be consulted.
14. Use secure methods when sharing or transmitting sensitive data. The approved method is CRA's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for CRA internal file transfer.
15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.
16. Limit use of individual data to the purposes that have been authorized within the scope of job responsibilities.

3.4 DATA SECURITY AND PRIVACY TRAINING

3.4.1 Purpose

CRA will provide a range of training opportunities for all CRA staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

3.4.2 Scope

All CRA board members, employees, and contracted partners.

3.4.3 Compliance

New employees that do not comply may not be able to use CRA networks or technology.

3.4.4 Policy

1. Within the first week of employment, all CRA board members, employees, and contracted partners must sign and follow the CRA Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. New employees that do not comply may not be able to use CRA networks or technology. Within the first week of employment, all CRA board members, employees, and contracted partners also must sign and obey the CRA Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current CRA board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this rule.
4. CRA requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data. The Chief Privacy Officer will identify these groups. Data and Statistics Coordinator will determine the annual training topics for these targeted groups based on CRA training needs.

5. Supervisors will annually monitor participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement. Supervisors and the board secretary will annually report all CRA board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

4 DATA DISCLOSURE

4.1 PURPOSE

Providing data to persons and entities outside of CRA increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This policy establishes the protocols and procedures for sharing data maintained by CRA. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99 and Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-303.

4.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

4.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by CRA are provided to CRA by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), CRA will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. CRA is not required to provide data that it does not maintain, nor is CRA required to create education records in response to an eligible student's request.

4.2.2 Third Party Vendor

Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with CRA must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-303. Vendors determined not to be compliant may not be allowed to enter into future contracts with CRA without third-party verification that they are compliant with federal and state law, and board rule.

4.2.3 Internal Partner Requests

Internal partners to CRA include school officials that are determined to have a legitimate educational interest in the information.

4.2.4 Governmental Agency Requests

CRA may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state

requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state

a) reporting requirement
b) audit
c) evaluation

The Coordinator of Data and Statistics will ensure the proper data disclosure avoidance are included if necessary.

4.3 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Coordinator of Data and Statistics will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules.

CRA may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

1. The CRA Principal, or board member, sponsors an external researcher or evaluator request.
2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Coordinator of Data and Statistics.
3. Researchers and evaluators supply the CRA a copy of any publication or presentation that uses CRA data 10 business days prior to any publication or presentation.

Process: Research Proposal must be submitted using this form: http://www.schools.utah.gov/data/Data-Request/ResearcherProposal.aspx. Research proposals are sent directly to the Student Data Managers for review. The IT Systems Security Manager may be consulted prior to a final decision.

5 Data breach

5.1 Purpose

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

5.2 Policy

CRA shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, CRA staff shall follow industry best practices outlined in the CRA IT Security Policy for responding to the breach. Further, CRA 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.

Concerns about security breaches must be reported immediately to the IT Security Manager who will collaborate with appropriate members of the CRA executive team to determine whether a security

breach has occurred. If the CRA Student Data Managers and IT Systems Security Manager determines that one or more employees or contracted partners have substantially failed to comply with CRA's Agency IT Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Manager must be reported immediately to the principal.

CRA will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach.

6 RECORD RETENTION AND EXPUNGEMENT

6.1 PURPOSE

Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

6.2 SCOPE

CRA board members and staff.

6.3 POLICY

The CRA staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53E-9-306, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53E-9-306, CRA shall expunge student data that is stored upon request of the student if the student is at least 23 years old. CRA may expunge medical records and behavioral test assessments. CRA will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. CRA staff will collaborate with Utah State Achieves and Records Services in updating data retention schedules.

CRA maintained student-level discipline data will be expunged after one year.

7 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

7.1 PURPOSE

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality at is addressed in five areas:

7.1.1 Data Governance Structure

The CRA data governance policy is structured to encourage the effective and appropriate use of educational data. The CRA data governance structure centers on the idea that data is the responsibility of all CRA sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

7.1.2 Data Collection

Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.

For all new data collections, CRA provides clear guidelines for data collection and the purpose of the data request.

7.1.3 Quality Control Checklist

Checklists have been proven to increase quality (See Appendix C). Therefore, before releasing high-risk data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

8 DATA TRANSPARENCY

Annually, CRA will publically post:

- CRA data collections
- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53E-9-303.