Renaissance Academy

Data Governance Plan

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. Renaissance Academy takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401 requires that Renaissance Academy adopt a Data Governance Plan.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, volunteers and contractors of Renaissance Academy. 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. This policy is designed to ensure only authorized disclosure of confidential information. The following 8 subsections provide data governance policies and processes for Renaissance Academy:

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

Furthermore, this Renaissance Academy Data Governance Plan works in conjunction with the school's Information Security Policy, which:

- Designates Renaissance Academy as the steward for all confidential information maintained within Renaissance Academy.
- Designates Data Stewards access for all confidential information.
- Requires Data Stewards to maintain a record of all confidential information for which they are responsible.
- 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 school data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Ensures that all Renaissance Academy 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.

3 DATA ADVISORY GROUPS

3.1 STRUCTURE

Renaissance Academy has a three-tiered data governance structure to ensure that data is protected at all levels of Utah's educational system.

3.2 GROUP MEMBERSHIP

Membership in the groups require board approval. Group membership is for two years. If individual members exit the group prior to fulfilling their two-year appointment, the board may authorize Renaissance Academy's Chief Officer to appoint a replacement member.

3.3 INDIVIDUAL AND GROUP RESPONSIBILITIES

The following tables outlines individual Renaissance Academy staff and advisory group responsibilities.

3.3.1 Table 1. Individual Renaissance Academy Staff Responsibilities

Role	Responsibilities
Executive Director	1. assumes primary LEA responsibility for legal, policy and procedural compliance with all data management obligations 2. ensures school wide compliance with all elements of the Renaissance Academy Data Governance Plan 3. investigates complains of alleged violations of security system and/or data data breaches 4. authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record
Data Manager	1. act as the primary local point of contact for the state student data officer 2. the 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 3. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation. 4. Create and maintain a list of all Renaissance staff that have access to personally identifiable student data. 5. Ensure annual school 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 data security systems laws throughout the school, including: a. providing training as part of user support b. producing resource materials, model plans, and model forms for LEA systems security annual report to the Executive Director of systems security needs

4 EMPLOYEE NON-DISCLOSURE ASSURANCES

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

4.1 SCOPE

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

4.2 NON-COMPLIANCE

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

4.3 NON-DISCLOSURE ASSURANCES

All student data utilized by Renaissance Academy is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way Renaissance Academy staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all Renaissance Academy staff to verify agreement to adhere to/abide by these practices and will be maintained in Renaissance Academy Human Resources. All Renaissance Academy 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 Renaissance Academy 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 Renaissance Academy 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 Renaissance Academy's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for Renaissance Academy 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 which have been authorized within the scope of job responsibilities.

4.4 DATA SECURITY AND PRIVACY TRAINING

4.4.1 Purpose

Renaissance Academy will provide a range of training opportunities for all Renaissance Academy 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.

4.4.2 Scope

All Renaissance Academy board members, employees, and contracted partners.

4.4.3 Compliance

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

4.4.4 Policy

1. Within the first week of employment, all Renaissance Academy board members, employees, and contracted partners must sign and follow the Renaissance Academy 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 Renaissance Academy networks or technology. Within the first week of employment, all Renaissance Academy board members, employees, and contracted partners also must sign and obey the Renaissance Academy Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current Renaissance Academy 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. Renaissance Academy 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 Renaissance Academy training needs.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by the Data Manager. The Data Manager will annually report all Renaissance Academy board members, employees, and contracted partners who do not have these requirements completed to the Executive Director.

5 DATA DISCLOSURE

5.1 PURPOSE

This policy establishes the protocols and procedures for sharing data maintained by Renaissance Academy. 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 §53A-1-1401.

5.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

5.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by Renaissance Academy may include both material generated by Renaissance Academy AND information provided to Renaissance Academy by the last school district of residence in which their student was enrolled. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), Renaissance Academy 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. Renaissance Academy is not required to provide data that it does not maintain, nor is Renaissance Academy required to create education records in response to an eligible student's request.

5.2.2 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 Renaissance Academy must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may not be allowed to enter into contracts with Renaissance Academy without third-party verification that they are compliant with federal and state law, and board rule.

5.2.3 Internal Partner Requests

Partners to Renaissance Academy include school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in writing and be reviewed and approved by the Executive Director.

Renaissance Academy will not disclose personally identifiable student information 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. Policy for External disclosure of Non-Personally Identifiable Information (PII)

5.3 Data Disclosure to a Requesting External Researcher or Evaluator

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

Renaissance Academy will 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.

6 Data breach

6.1 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.

6.2 Policy

Renaissance Academy shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, Renaissance Academy staff shall follow industry best practices outlined in the IT Security Policy for responding to the breach. Further, Renaissance Academy 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 Executive Director who will collaborate with appropriate members of the Renaissance Academy executive team to determine whether a security breach has occurred. If the Renaissance Academy data breach response team determines that one or more employees or contracted partners have substantially failed to comply with Renaissance Academy's 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 Executive Director.

7 Record retention and expungement

7.1 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.

7.2 Scope

Renaissance Academy board members and staff.

7.3 POLICY

Renaissance Academy shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53A-1-1407, Renaissance Academy shall expunge student data that is stored upon request of the student if the student is at least 23 years old. Renaissance Academy may expunge medical records and behavioral test assessments. Renaissance Academy will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. Renaissance Academy staff will collaborate with Utah State Achives and Records Services in updating data retention schedules.

Renaissance Academy maintained student-level discipline data will be expunged after three years.

8 QUALITY ASSURANCES AND TRANSPARENCY REQUIREMENTS

8.1 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:

8.1.1 Data Governance Structure

The Renaissance Academy data governance policy is structured to encourage the effective and appropriate use of educational data. The Renaissance Academy data governance structure is built on two important principals 1) that data security and individual privacy rights are the responsibility of all Renaissance Academy board members, administration, faculty and staff and 2) that data driven decision making is the goal of all data collection, storage, reporting and analysis.

8.1.2 Data Requirements and Definitions

The Utah State Board of Education (USBE) communicates data requirements and definitions to Renaissance Academy through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). USBE will communicate with Renaissance Academy 's data managers regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Whenever applicable, Renaissance Academy program specialists and program directors may also attend these meetings.

8.1.3 Data Collection

It is highly recommended that whenever possible, data is collected at the lowest level available (i.e. at the student/teacher level) and that the number of collections be as few as possible to minimize potential breaches of data security. Two examples of this practice are: 1) file sharing tools such as secured folders or cloud sharing such as Google docs should be used in order to minimize the number of electronic files generated 2) data should be gathered and maintained at the most detailed level therefore aggregate data can be derived or calculated from the detailed data. This minimizes the number people involved and the number of times sensitive information is accessed. Both of which provide opportunity for potential security breaches.

8.1.4 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.

9 DATA TRANSPARENCY

Annually, Renaissance Academy will publically post:

- Renaissance Academy's data collections
- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

10 APPENDIX

Appendix A. Renaissance Academy Employee Non-Disclosure Agreement

As an employee of the Renaissance Academy, I hereby affirm that: (Initial)

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan Renaissance Academy policies. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the Renaissance Academy's policies and its subordinate process and procedures;

_____ I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or videotape images, of your attempts to access the facility and/or workstations.

Trainings

_____ I have completed Renaissance Academy's Data Security and Privacy Fundamentals Training.

_____ I will complete Renaissance Academy's Data Security and Privacy Fundamentals Training within 30 days.

Using Renaissance Academy Data and Reporting Systems

_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, for either personal computer(s) or Renaissance Academy system user accounts, with Renaissance Academy staff or participating program staff.

_____I will log out of and close the browser after each use of Renaissance Academy data and reporting systems.

_____I will only access data in which I have received explicit written permissions from the data owner.

_____I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data;

Handling Sensitive Data

_____ I will keep sensitive data on password-protected school-authorized computers.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records should be used for such presentations.

_____ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured Renaissance Academy server.

Reporting & Data Sharing

_____ I will not redisclose or share any confidential data analysis except to other authorized personnel without Renaissance Academy's expressed written consent.

_____ I will not publically publish any data without the approval of the Executive Director.

_____ I will take steps to avoid disclosure of personally identifiable information in school-level reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____I will not transmit child/staff-level data externally unless explicitly authorized in writing by the Executive Director.

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or Renaissance Academy's Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for Renaissance Academy internal file transfer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to the Executive Director. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

Consequences for Non-Compliance

_____ I understand that access to the Renaissance Academy network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

_____I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

_____I agree that upon the cessation of my employment from Renaissance Academy, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Renaissance Academy without the prior written permission of the Executive Director of Renaissance Academy.

Print Name: _____

Signed: _____

Date: _____

Approved 9-20-17