Bonneville Academy Data Governance Plan

Official Policies and Procedures of the *Bonneville Academy*	
Effective/Revision Date: 1/2/2018	
Policy Title: *Bonneville 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. *Bonneville 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 *Bonneville Academy* adopt a Data Governance Plan.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, and contractors of the Agency. 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 Agency 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 8 subsections provide data governance policies and processes for *Bonneville 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 *Bonneville Academy* Data Governance Plan works in conjunction with the Agency Information Security Policy, which:

· Designates *Bonneville Academy* as the steward for all confidential information maintained within *Bonneville Academy*.

· 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 *Bonneville Academy* standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all *Bonneville 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

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

. It is the objective of the Bonneville Academy Board of Directors and School Administration to provide reliable, efficient information systems services for all business and student administrative functions. The Technology Committee shall make recommendations that will establish and maintain an efficient and economical computer system, as the budget and current technology will permit. Installation, connection and integration of information systems shall be performed by the contracted information systems party and/or staff authorized by the Board of Directors, and must have the approval of the director and Technology Committee.

The director and staff shall also review proposed machines, materials and methods of handling data used by an administrative unit to ensure compatibility with the LEA system and policies, as well as following state and federal policies and law.. The Technology Committee shall advise LEA personnel on methods, feasibility and costs for data handling and for future plans.

The contracted information systems party shall implement steps to provide appropriate security procedures and in so doing shall:

1. Suggest ways to Establish and supervise procedures that keep data secure against misuse and unauthorized access.
2. Release data only to the school administration or designee responsible for the use and dissemination of the data, in accordance with FERPA regulations.
3. Protect stored data against loss by maintaining appropriate backup systems.
4. Train administrators in security procedures.
5. Correct procedures that threaten or weaken the security of data.
6. Report breaches of security to the administrator, who will then report to the school board and Technology Committee.
7. Suggest ways to Establish and maintain proper security procedures within the physical facilities to protect the equipment against all reasonable sources of disaster and unauthorized access.
8. Develop and maintain a disaster recovery plan.

The contracting information systems party shall:

1. Establish and maintain a LEA communication network so that all legitimate users may have access to only the necessary information that is appropriate for their assignment.
2. Provide and maintain an electronic mail system.
3. Direct and coordinate the use of microcomputers in LEA administrative functions.
4. Establish convenient and efficient submial and retrieval procedures.
5. Process each unit's data accurately and on a monthly basis.
6. Provide appropriate training for operators, administrators and other staff in the effective use of information systems.

7. Troubleshoot interruptions of service to the LEA , restoring all malfunctioning equipment to service as soon as possible. When necessary, provide alternative procedures during malfunctions to assure support to all units.

8. Make recommendations to director when there is an appropriate need for consulting services.

9. Monitor the quality of data processing work to reduce errors from all sources.

The contracting information systems party shall provide and/or arrange for adequate maintenance for all mainframe related equipment. The contracting information systems party shall advise the director of the need for changes to network/information systems, providing pertinent information such as hardware/software solutions, performance and maintenance problems. The contracting information systems party shall perform other dues as assigned by the school administration, following recommendations from the Technology Committee.

3.2 Group Membership

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

3.3 Individual and Group Responsibilities

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

Role	Responsibilities

LEA 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 have 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: 1. providing training and support to applicable *Bonneville Academy* employees; and 2. 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 *Bonneville Academy*'s systems security needs
Educators	

Other	

3.3.1 Table 1. Individual *Bonneville Academy* Staff Responsibilities

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 *Bonneville Academy* board members, employees, contractors and volunteers must sign and obey the *Bonneville 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 *Bonneville 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 *Bonneville Academy* is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way *Bonneville Academy* staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all *Bonneville Academy* staff to verify agreement to adhere to/abide by these practices and will be maintained in *Bonneville Academy* Human Resources. All *Bonneville 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 requested by the Student Data Manager.

3. Consult with *Bonneville Academy* internal data owners when creating or disseminating reports containing data.
4. Use password-protected LEA-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 *Bonneville Academy* when disposing of such records.
9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate student/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 *secure, password protected email.*
15. NOT transmit student/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

Bonneville Academy will provide a range of training opportunities for all *Bonneville 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 *Bonneville Academy* board members, employees, and contracted partners.

4.4.3 Compliance

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

4.4.4 Policy

1. Within the first week of employment, all *Bonneville Academy* board members, employees, and contracted partners must sign and follow the *Bonneville 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 *Bonneville Academy* networks or technology. Within the first week of employment, all *Bonneville Academy* board members, employees, and contracted partners also must sign and obey the *Bonneville Academy* Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current *Bonneville 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. *Bonneville 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 Student Data Manager will identify these groups and will determine the annual training topics for these targeted groups based on *Bonneville 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 supervisors. Supervisors and the board secretary will annually report all *Bonneville Academy* board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

5 Data disclosure

5.1 Purpose

Providing data to persons and entities outside of the *Bonneville Academy* increases transparency, promotes education in *Bonneville Academy*, and increases knowledge about Utah public education. This policy establishes the protocols and procedures for sharing data maintained by *Bonneville 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

In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), *Bonneville Academy* will provide parents with access to their student'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. *Bonneville Academy* is not required to provide data that it does not maintain, nor is *Bonneville 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 *Bonneville 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 future contracts with *Bonneville Academy* without third-party verification that they are compliant with federal and state law and board rule.

5.2.3 Internal Partner Requests

Internal partners to *Bonneville Academy* include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in *Bonneville Academy*'s *Data Officer.*

5.2.4 Governmental Agency Requests

Bonneville Academy 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 Student Data Manager will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

5.3 Policy for External disclosure of Non-Personally Identifiable Information (PII)

5.3.1 Scope

External data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

5.3.2 Student Data Disclosure Risk Levels

Bonneville Academy has determined four levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Student Data Manager will make final determinations on classification of student data requests risk level.

5.3.2.1 Low-Risk Data Request Process

Definition: High-level aggregate data
Examples:

- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

Process: Requests will be made in writing to Data Manager and Administration, intent and purpose must be shared. Appropriate forms will be completed.

5.3.2.2 Medium-Risk Data Request Process

Definition: Aggregate data, but because of potentially low n-sizes, the data must have disclosure avoidance methods applied.

Examples:

- Graduation rate by year and LEA
- Percent of third-graders scoring proficient on the SAGE ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

Process: Requests will be made in writing to Data Manager and Administration, intent and purpose must be shared. Appropriate forms will be completed.

5.3.2.3 High-Risk Data Request Process

Definition: Student-level data that are de-identified.

Examples:

- De-identified student-level graduation data
- De-identified student-level SAGE ELA assessment scores for grades 3-6.

Process: Requests will be made in writing to Data Manager and Administration, intent and purpose must be shared. Appropriate forms will be completed.

5.4 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Student Data Manager will ensure the proper data are shared with external researcher or evaluator to comply with federal, state, and board rules.
Bonneville Academy 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. A *Bonneville Academy* Director, Superintendent, 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 Student Data Management.
3. Researchers and evaluators supply the *Bonneville Academy* a copy of any publication or presentation that uses *Bonneville Academy* data 10 business days prior to any publication or presentation.

Process: Requests will be made in writing to Data Manager and Administration, intent and purpose must be shared. Appropriate forms will be completed.

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

Bonneville 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, *Bonneville Academy* staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, *Bonneville 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 IT security manager who will collaborate with appropriate members of the *Technology Committee* to determine whether a security breach has occurred. If the *Bonneville Academy* data breach response team determines that one or more employees or contracted partners have substantially failed to comply with *Bonneville Academy*'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 Superintendent.

Bonneville Academy will provide and periodically update, in keeping with industry best practices, resources for LEA staff, faculty, and volunteers in preparing for and responding to a security breach. *Bonneville Academy* will make these resources available on its website.

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

Bonneville Academy board members and staff.

7.3 Policy

The *Bonneville Academy*, staff, and schools 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, the *Bonneville Academy* shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The *Bonneville*

Academy may expunge medical records and behavioral test assessments. *Bonneville Academy* will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. *Bonneville Academy* staff will collaborate with *Utah State Archives and Records Services and USBE* in updating data retention schedules.
Bonneville 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 *Bonneville Academy* data governance policy is structured to encourage the effective and appropriate use of educational data. The *Bonneville Academy* data governance structure centers on the idea that data is the responsibility of all *Bonneville Academy* 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.

8.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, *Bonneville Academy* communicates data requirements and definitions through the school website. *Bonneville Academy* also communicates with LEA IT staff regularly, at *monthly professional development meetings and data dives.* Where possible, *Bonneville Academy* program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.
On the data reporting side, the production and presentation layers provide standard data definitions and business rules. *All FERPA rules and regulations are followed, and training occurs annually for all school employees.*

8.1.3 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, *Bonneville Academy* provides clear guidelines for data collection and the purpose of the data request. The *Bonneville Academy* also notifies stakeholders as soon as possible about future data collections.

8.1.4 Data Auditing

Our external IT company will perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies.

8.1.5 Quality Control Checklist

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

9 Data Transparency

Annually, *Bonneville Academy* will publically post:

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

10 Appendix

Appendix A. *Bonneville Academy* Employee Non-Disclosure Agreement/Employee Technology Agreement
Every Bonneville Academy employee will be required to sign this Technology Agreement each school year. Computer and network use are necessary components of an employee's work at Bonneville Academy. In addition, varying work responsibilities result in access to information sources such as software, programs, the internet, school network, etc. Although employees may have access to these information sources, their use must be specially authorized.
Access and authorization to information and equipment carry a corresponding responsibility for their appropriate use. School equipment and access are intended to be used for educational and professional/career development activities. Expectations of employees include, but are not limited to, the following (see {ELECTRONIC INFORMATION RESOURCES AND ACCEPTABLE USE} for a full listing of acceptable and unacceptable activities):

1. Student Personal Safety

a. Employees who supervise students with access to technology equipment shall be familiar with the Bonneville Academy Student Technology Use Agreement and enforce its provisions.

b. All student technology use must be supervised by a teacher who has signed this agreement.

2. Student Information and Records

a. Student data on the SIS, other databases, or simply gathered by educators are educational records for the purposes of FERPA and are protected as are other educational records.

b. Employees are responsible to meet the requirements of FERPA prior to the release or dissemination of any educational records, including student data, whether aggregated or disaggregated.

. Employees are responsible to prevent disclosure of information or data in their control. This includes removable media and portable devices (e.g.: laptops, flash drives, etc.).

3. Illegal or Destructive Activities

a. Employees shall not go beyond their authorized access to the school network or other computer equipment or software including the files or accounts of others.

b. Employees shall not disrupt or attempt to damage or disrupt technology equipment or systems, including acvies that would affect data or system performance.

c. Employees shall not use School equipment to engage in illegal acts.

4. System Security

a. Employees are responsible for the security of their technology equipment, files and passwords.

b. Employees shall promptly notify the School of security problems.

c. Employees with access to student records may not use, release, or share these records except as authorized by Federal and State law.

d. Students may not have access to technology equipment other than workstations.

e. Staff will not leave their workstations unlocked or devices unattended while logged into the network.

f. Passwords are to be protected and not shared with anyone. This applies to students who are teacher aides and family members of staff.

5. Inappropriate Conduct—the following are prohibited in public, private or posted messages or files:

a. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language;

b. Potentially damaging, dangerous or disruptive material;

c. Personal or generalized attacks or harassment; and

d. False or defamatory information.

6. Plagiarism and Copyright Infringement

a. Works may not be plagiarized.

b. The rights of copyright owners are to be respected. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that is protected by copyright, the expressed requirements should be followed. If an employee is unsure whether or not a work can be used, the copyright owner should be contacted for permission.

c. Software copyrights must be strictly respected.

7. Inappropriate Access to Material

a. School equipment shall not be used with material that is profane, obscene (pornographic) or advocates illegal acts, violence or discrimination. This restriction applies regardless of the physical location of equipment and regardless of network being used.

b. The non-educational use of mul-player computer games on school equipment is not allowed. This restriction applies to family members of staff.

c. Inadvertent inappropriate access shall be reported immediately to the principal or supervisor.

8. Expectation of Privacy

a. Employees have no expectation of privacy in files, disks, documents, etc., which have been created in, entered in, stored in, downloaded from, or used on School equipment.

9. Services and Assumption of Risks

a. The School makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the system to include loss of data and inaccurate or poor quality information obtained from the system.

10. All acceptable and unacceptable activities as listed in [ELECTRONIC INFORMATION RESOURCES AND ACCEPTABLE USE]

11. Due Process

a. In the event there is an allegation that an employee has violated this agreement, the employee will receive notice of the alleged violation and an opportunity to present an explanation. b. Disciplinary actions in harmony with Corrective Discipline procedures will be tailored to meet the specific concerns related to the violation. Deliberate violations of this agreement (e.g. malicious acts or omissions; searching for, viewing or otherwise visiting pornographic or sexually explicit sites) are cause for immediate termination.

I have read and understand this document and the Electronic Information Resources and Acceptable Use policy and its provisions. Employee Computer Use Agreement and its provisions. I understand that violation of this Agreement are grounds for discipline and may be cause for immediate termination.

Name_____
_ (last, first, middle)

Grade/Subject/Department_____School/Locaon_____
_____ _____

Signature_____Date_____
_____ _____

Appendix B. Protecting PII in Public Reporting

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by Bonneville Academy is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school or LEA -level reports.

This is done by applying the following statistical method for protecting PII.

1. Underlying counts for groups or subgroups totals are not reported.
2. If a reporting group has 1 or more subgroup(s) with 10 or fewer students.
    - The results of the subgroup(s) with 10 or fewer students are recorded as "N<10"
    - For remaining subgroups within the reporting group
        1. For subgroups with 300 or more students, apply the following suppression rules.
            1. Values of 99% to 100% are recorded to ≥99%
            2. Values of 0% to 1% are recorded to ≤1%
        2. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
            1. Values of 98% to 100% are recorded to ≥98%
            2. Values of 0% to 2% are recorded to ≤2%
        3. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
            1. Values of 95% to 100% are recorded to ≥95%
            2. Values of 0% to 5% are recorded to ≤5%
        4. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
            1. Values of 90% to 100% are recorded to ≥90%
            2. Values of 0% to 10% are recorded to ≤10%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)
        5. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.
            1. Values of 80% to 100% are recorded to ≥80%
            2. Values of 0% to 20% are recorded to ≤20%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

Appendix C. Quality Control Checklist

Reliability (results are consistent)

1. Same definitions were used for same or similar data previously reported **or** it is made very clear in answering the request how and why different definitions were used
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another *Bonneville Academy* data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

1. Request was clarified
2. Identified and included all data owners that would have a stake in the data used
3. Data owners approve of data definitions and business rules used in the request
4. All pertinent business rules were applied
5. Data answers the intent of the request (intent ascertained from clarifying request)
6. Data answers the purpose of the request (audience, use, etc.)
7. Limits of the data are clearly stated
8. Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

1. Is date-stamped
2. Small n-sizes and other privacy issues are appropriately handled
3. Wording, spelling, and grammar are correct
4. Data presentation is well organized and meets the needs of the requester
5. Data is provided in a format appropriate to the request
6. A typical person could not easily misinterpret the presentation of the data