



## 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. *Beehive Science and Technology 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 *Beehive Science and Technology 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 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 *Beehive Science and Technology 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 *Beehive Science and Technology Academy* Data Governance Plan works in conjunction with the Agency Information Security Policy, which:

- Designates *Beehive Science and Technology Academy* as the steward for all confidential information maintained within *Beehive Science and Technology Academy*.
- Designates Data Steward's 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 *Beehive Science and Technology Academy* standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all *Beehive Science and Technology Academy* board members, employees, contractors, and volunteers comply with the policy and undergo 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

*Beehive Science and Technology Academy* has a three-tiered data governance structure to ensure that data is protected at all levels.

### 3.2 GROUP MEMBERSHIP

Membership in the groups will be for two years. Administrators, teachers, and parents may join the group. If individual members exit the group prior to fulfilling their two-year term, the *Beehive Science and Technology Academy's* Chief Officer will appoint a replacement member.

### 3.3 INDIVIDUAL AND GROUP RESPONSIBILITIES

The following table outlines individual *Beehive Science and Technology Academy* staff and advisory group responsibilities.

Role	Responsibilities
<b>LEA Student Data Manager</b>	<ol style="list-style-type: none"> <li>1. authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity</li> <li>2. act as the primary local point of contact for the state student data officer.</li> <li>3. A student data manager may share personally identifiable student data that are: <ol style="list-style-type: none"> <li>a. of a student with the student and the student's parent</li> <li>b. required by state or federal law</li> <li>c. in an aggregate form with appropriate data redaction techniques applied</li> <li>d. for a school official</li> <li>e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court</li> <li>f. in response to a subpoena issued by a court.</li> <li>g. directory information</li> <li>h. submitted data requests from external researchers or evaluators,</li> </ol> </li> <li>4. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation.</li> <li>5. Create and maintain a list of all LEA staff that have access to personally identifiable student data.</li> <li>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.</li> </ol>
<b>IT Systems Security Manager</b>	<ol style="list-style-type: none"> <li>1. Acts as the primary point of contact for state student data security administration in assisting the board to administer this part;</li> <li>2. ensures compliance with security systems laws throughout the public education system, including: <ol style="list-style-type: none"> <li>a. providing training and support to applicable <i>Beehive Science and Technology Academy</i> employees; and</li> <li>b. producing resource materials, model plans, and model forms for LEA systems security;</li> </ol> </li> <li>3. investigates complaints of alleged violations of systems breaches;</li> <li>4. provides reports to the board on <i>Beehive Science and Technology Academy's</i> systems security needs</li> </ol>
<b>Educators</b>	
<b>Other</b>	

### 3.3.1 Table 1. Individual {*Beehive Science and Technology 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 *Beehive Science and Technology Academy* board members, employees, contractors and volunteers must sign and obey *Beehive Science and Technology Academy* Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of school technology and information.

### 4.2 NON-COMPLIANCE

Non-compliance with the agreements shall result in consequences up to and including removal of access to *Beehive Science and Technology 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 *Beehive Science and Technology Academy* is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way *Beehive Science and Technology Academy* staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all *Beehive Science and Technology Academy* staff to verify agreement to adhere to/abide by these practices and will be maintained in *Beehive Science and Technology Academy* Human Resources. All *Beehive Science and Technology Academy* employees (including permanent or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Consult with *Beehive Science and Technology Academy* internal data owners when creating or disseminating reports containing data.
3. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
4. NOT share individual passwords for personal computers or data systems with anyone.
5. Log out of any data system/portal and close the browser after each use.
6. 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.

7. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at *Beehive Science and Technology Academy* when disposing of such records.
8. 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.
9. 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).
10. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
11. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
12. 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.
13. Use secure methods when sharing or transmitting sensitive data.
14. 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.
15. 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**

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

### **4.4.3 Compliance**

New employees that do not comply may not be able to use *Beehive Science and Technology Academy* networks or technology.

### **4.4.4 Policy**

1. Within the first week of employment, all *Beehive Science and Technology Academy* board

members, employees, and contracted partners must sign and follow the *Beehive Science and Technology 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 *Beehive Science and Technology Academy* networks or technology. Within the first week of employment, all *Beehive Science and Technology Academy* board members, employees, and contracted partners also must sign and obey the *Beehive Science and Technology Academy* Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current *Beehive Science and Technology Academy* board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 100 days of the adoption of this rule.
4. *Beehive Science and Technology 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 *Beehive Science and Technology 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 *Beehive Science and Technology 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 *Beehive Science and Technology Academy* 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 *Beehive Science and Technology 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 of their students are maintained by *Beehive Science and Technology Academy*, and access to their student's record can be obtained from the school. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), LEAs 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. LEAs and *Beehive Science and Technology Academy* is not required to provide data that it does

not maintain, nor is *Beehive Science and Technology 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 *Beehive Science and Technology 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 *Beehive Science and Technology 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 *Beehive Science and Technology Academy* include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in *Beehive Science and Technology Academy's* data request ticketing system.

### **5.2.4 Governmental Agency Requests**

*Beehive Science and Technology 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 Coordinator of Data and Statistics 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**

*Beehive Science and Technology 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 Coordinator of Data and Statistics 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 sixth-graders scoring proficient on the SAGE ELA assessment

Process: Requester creates a ticket, Data Request forwarded to appropriate Data Steward. Data Steward fulfills request and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket.

#### **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 sixth-graders scoring proficient on the SAGE ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

Process: Requester creates a ticket, Data Request forwarded to appropriate Data Steward, Data Steward fulfills request, applies appropriate disclosure avoidance techniques, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

#### **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: Requester creates a ticket, Data Request forwarded to Data Coordinator for review. If the request is approved, an MOA is drafted and sent to Administration, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate. If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.



## 5.4 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.

*Beehive Science and Technology 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 *Beehive Science and Technology 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 Coordinator of Data and Statistics.
3. Researchers and evaluators supply the *Beehive Science and Technology Academy* a copy of any publication or presentation that uses *Beehive Science and Technology Academy* data 10 business days prior to any publication or presentation.

Process: Research Proposal must be submitted to Administration: Research proposals are sent directly to the Coordinator of Data and Statistics for review. If the request is approved, an MOA is drafted and sent to Director, sent to the Purchasing/Contract Manager, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate. If it passes QA, data are sent to requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data are sent back to the Data Steward for modification.

## 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

*Beehive Science and Technology 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, *Beehive Science and Technology Academy* staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, *Beehive Science and Technology 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 *Beehive Science and Technology Academy* executive team to determine whether a security breach has occurred. If *Beehive Science and Technology Academy* data breach response team determines that one or more employees or contracted partners have substantially failed to comply with *Beehive Science and Technology 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 Director.

*Beehive Science and Technology Academy* will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach.

## **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**

*Beehive Science and Technology Academy* board members and staff.

### **7.3 POLICY**

The *Beehive Science and Technology Academy*, staff 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 *Beehive Science and Technology Academy* shall expunge student data that is stored upon request of the student if the student is at least 23 years old. *Beehive Science and Technology Academy* may expunge medical records and behavioral test assessments. *Beehive Science and Technology Academy* will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. *Beehive Science and Technology Academy* staff will collaborate with Utah State Archives and Records Services in updating data retention schedules.

*Beehive Science and Technology 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 is addressed in five areas:

### **8.1.1 Data Governance Structure**

The *Beehive Science and Technology Academy* data governance policy is structured to encourage the effective and appropriate use of educational data. The *Beehive Science and Technology Academy* data governance structure centers on the idea that data is the responsibility of all *Beehive Science and Technology 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, the *Beehive Science and Technology Academy* communicates data requirements and definitions to LEAs staff. *Beehive Science and Technology Academy* also communicates with LEA IT staff regularly. Where possible, *Beehive Science and Technology 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. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped.

### **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, *Beehive Science and Technology Academy* provides to staff clear guidelines for data collection and the purpose of the data request.

### **8.1.4 Data Auditing**

Data and Statistics Data Analysts 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. Data Analysts also work with School Finance Department to address findings from the Auditors.

### **8.1.5 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

---

*Beehive Science and Technology Academy* will publically post:

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

## 10 APPENDIX

---

### Appendix A. *Beehive Science and Technology Academy* Employee Non-Disclosure Agreement

#### **As an employee of *Beehive Science and Technology 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 *Beehive Science and Technology Academy* policies. These assurances address general procedures, data use/sharing, and data security.

\_\_\_\_\_ I will abide by the terms of the *Beehive Science and Technology 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 *Beehive Science and Technology Academy's* Data Security and Privacy Fundamentals Training.

\_\_\_\_\_ I will complete *Beehive Science and Technology Academy's* Data Security and Privacy Fundamentals Training within 60 days.

#### **Using *Beehive Science and Technology 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 *Beehive Science and Technology Academy* system user accounts, with *Beehive Science and Technology Academy* staff or participating program staff.

\_\_\_\_\_ I will log out of and close the browser after each use of *Beehive Science and Technology 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 state-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 *Beehive Science and Technology Academy* server.

## Reporting & Data Sharing

- \_\_\_\_\_ I will not re-disclose or share any confidential data analysis except to other authorized personnel without *Beehive Science and Technology Academy's* expressed written consent.
- \_\_\_\_\_ I will not publically publish any data without the approval of the Director.
- \_\_\_\_\_ I will take steps to avoid disclosure of personally identifiable information in state-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.
- \_\_\_\_\_ I understand that when sharing child/staff-identifying data with authorized individuals, I will use *Beehive Science and Technology Academy's* Secure File Transfer Protocol. Also, sharing within secured server folders is appropriate for *Beehive Science and Technology Academy* internal file transfer.
- \_\_\_\_\_ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and *Beehive Science and Technology Academy* Information Security Officer. 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 *Beehive Science and Technology 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 *Beehive Science and Technology Academy*, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of *Beehive Science and Technology Academy* without the prior written permission of the Student Data Manager of *Beehive Science and Technology Academy*.

Print Name: \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

## Appendix B. Protecting PII in Public Reporting

### Data Gateway Statistical Reporting Method for Protecting PII

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 the *staff* and Beehive Academy is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

## Appendix C. Example 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 *Beehive Science and Technology 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)

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

### Presentation

13. Is date-stamped
14. Small n-sizes and other privacy issues are appropriately handled
15. Wording, spelling and grammar are correct
16. Data presentation is well organized and meets the needs of the requester
17. Data is provided in a format appropriate to the request
18. A typical person could not easily misinterpret the presentation of the data