1. Governing Principles

Beehive Science & Technology Academy (referred to as Beehive Science & Technology Academy throughout) takes its responsibility toward student data seriously. This governance plan incorporates the following Generally Accepted Information Principles (GAIP):

Risk: There is risk associated with data and content. The risk must be formally recognized, either as a liability or through incurring costs to manage and reduce the inherent risk.
Due Diligence: If a risk is known, it must be reported. If a risk is possible, it must be confirmed.
Audit: The accuracy of data and content is subject to periodic audit by an independent body.
Accountability: An organization must identify parties which are ultimately responsible for data and content assets.
Liability: The risks in information means there is a financial liability inherent in all data or content that is based on regulatory and ethical misuse or mismanagement.

2. Data Maintenance and Protection Policy

Beehive Science & Technology Academy recognizes that there is risk and liability in maintaining student data and other education-related data and will incorporate reasonable data industry best practices to mitigate this risk.

2.1 Process

In accordance with R277-487, Beehive Science & Technology Academy shall do the following:

Designate an individual as an Information Security Officer
Adopt the CIS Controls or comparable
Report to the USBE by October 1 each year regarding the status of the adoption of the CIS controls or comparable and future plans for improvement.

3. Roles and Responsibilities Policy

Beehive Science & Technology Academy acknowledges the need to identify parties who are ultimately responsible and accountable for data and content assets. These individuals and their responsibilities are as follows:

3.1 Data Manager roles and responsibilities

authorize and manage the sharing, outside of the student data manager's education entity, of personally identifiable student data for the education entity as described in this section
provide for necessary technical assistance, training, and support
act as the primary local point of contact for the state student data officer
ensure that the following notices are available to parents:

- annual FERPA notice (see 34 CFR 99.7
- directory information policy (see 34 CFR 99.37
- survey policy and notice (see 20 USC 1232h and 53E-9-203
- data collection notice (see 53E-9-305

3.2 Information Security Officer

Oversee adoption of the CIS controls

Provide for necessary technical assistance, training, and support as it relates to IT security

4. Training and Support Policy

Beehive Science & Technology Academy recognizes that training and supporting educators and staff regarding federal and state data privacy laws is a necessary control to ensure legal compliance.

4.1 Procedure

The data manager will ensure that educators who have access to student records will receive an annual training on confidentiality of student data to all employees with access to student data. The content of this training will be based on the Data Sharing Policy.

By October 1 each year, the data manager will report to USBE the completion status of the annual confidentiality training and provide a copy of the training materials used.

The data manager shall keep a list of all employees who are authorized to access student education records after having completed a training that meets the requirements of 53E-9-204

Beehive Science & Technology Academy assures that Training and Support is provided by the following process:

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. Audit Policy

In accordance with the risk management priorities of Beehive Science & Technology Academy, Beehive Science & Technology Academy will conduct an audit of:

The effectiveness of the controls used to follow this data governance plan; and
Third-party contractors, as permitted by the contract described in 53E-9-309(2).

6. Data Sharing Policy

There is a risk of re-disclosure whenever student data are shared. Beehive Science & Technology Academy shall follow appropriate controls to mitigate the risk of re-disclosure and to ensure compliance with federal and state law.

6.1 Procedure

The data manager shall approve all data sharing or designate other individuals who have been trained on compliance requirements with FERPA.

For external research, the data manager shall ensure that the study follows the requirements of FERPA's study exception described in 34 CFR 99.31(a)(6).

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 researchers 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-identified data as appropriate. If it passes QA, data are sent to the requester and saves the data set 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.

After sharing from student records, the data manager shall ensure that an entry is made in Beehive Science & Technology Academy Metadata Dictionary to record that the exchange happened.
After sharing from student records, the data manager shall make a note in the student record of the exchange in accordance with 34 CFR 99.32

7. Expungement Request Policy

Beehive Science & Technology Academy recognizes the risk associated with data following a student year after year that could be used to mistreat the student. Beehive Science & Technology Academy shall review all requests for records expungement from parents and make a determination based on the following procedure.

7.1 Procedure

The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.

If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
Beehive Science & Technology Academy shall decide whether to expunge the data within a reasonable time after the request.
If Beehive Science & Technology Academy decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
Beehive Science & Technology Academy shall hold the hearing within a reasonable time after receiving the request for a hearing.
Beehive Science & Technology Academy shall provide the parent notice of the date, time, and place in advance of the hearing.
The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
Beehive Science & Technology Academy shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
Beehive Science & Technology Academy shall make its decision in writing within a reasonable time following the hearing.
The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.
If the decision is to expunge the record, Beehive Science & Technology Academy will seal it or make it otherwise unavailable to other staff and educators.

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. Data Breach Response Policy

Beehive Science & 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 & Technology Academy staff shall follow industry best practices for responding to the breach.

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.

8.1 Procedures

The superintendent/director will work with the information security officer to designate individuals to be members of the cyber incident response team (CIRT)

At the beginning of an investigation, the information security officer will begin tracking the incident and log all information and evidence related to the investigation.

The information security officer will call the CIRT into action once there is reasonable evidence that an incident or breach has occurred.

The information security officer will coordinate with other IT staff to determine the root cause of the breach and close the breach.

The CIRT will coordinate with legal counsel to determine if the incident is meets the legal definition of a significant breach as defined in R277-487 and determine which entities and individuals need to be notified.

If law enforcement is notified and begins an investigation, the CIRT will consult with them before notifying parents or the public so as to not interfere with the law enforcement investigation.

9. Publication Policy

Beehive Science & Technology Academy recognizes the importance of transparency and will post this policy on Beehive Science & Technology Academy website.