Official Policies and Procedures of Spectrum Academy	
Effective/Revision Date: 9/15/2021	
Policy Title: Spectrum 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. The Utah Board of Education and Spectrum 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 Spectrum Academy adopt a Data Governance Plan.

2 SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, vendors, and contractors of Spectrum 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. In accordance with Spectrum Academy 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 eight subsections provide data governance policies and processes for Spectrum 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 Spectrum Academy Data Governance Plan works in conjunction with the Spectrum Academy Information Security Policy, which:

- Designates Spectrum Academy as the steward for all confidential information maintained within Spectrum 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 Spectrum Academy 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 Spectrum Academy's standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all Spectrum Academy board of director's ("Board") members, employees, vendors, 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
Spectrum 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 Spectrum Academy's Academic Director to appoint a replacement member.

3.3 INDIVIDUAL AND GROUP RESPONSIBILITIES
The following tables outlines individual Spectrum Academy staff and advisory group responsibilities.

3.3.1 Table 1. Individual Spectrum Academy Staff 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/or (as applicable) the student's parent consent
	    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:
	    a. providing training and support to applicable Spectrum Academy employees; and
	    b. producing resource materials, model plans, and model forms for LEA systems security.
	3. Investigates complaints of alleged violations of systems breaches.
	4. Provides an annual report to the Board on Spectrum Academy's systems security needs

Educators	
Other	

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

3. Consult with Spectrum 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 Spectrum 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 Spectrum Academy's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for 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
Spectrum Academy will provide a range of training opportunities for all staff, including volunteers, vendors, 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 Spectrum Academy Board members, employees, vendors and contracted partners.

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

4.4.4 Policy
1. Within the first week of employment, all Spectrum Academy Board members, employees, and contracted partners must sign and follow the 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 Spectrum Academy networks or technology. Within the first week of employment, all Board members, employees, and contracted

partners also must sign and obey the Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.

3. All current Spectrum Academy Board members, employees, vendors 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. Spectrum 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 staff 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 Director of Academics will annually report all Spectrum Academy Board members, employees, vendors 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 Spectrum 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 Spectrum 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 Spectrum Academy are provided to the campus in which their student is/was enrolled, and access to their student's record can be obtained from the student's specific school campus. 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. Spectrum Academy is not required to provide data that it does not maintain, nor is 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, functions.

All third-party vendors contracting with Spectrum 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 Spectrum 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 Spectrum Academy include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in the data request ticketing system.

5.2.4   Governmental Agency Requests

Spectrum 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

Spectrum Academy has determined three 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 third-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 third-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 and Statistic Coordinator for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the Director, sent to the Purchasing/Contract Manager, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills request, de-identifies data as appropriate, 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. 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.

Spectrum 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 Spectrum Academy Director 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 Spectrum Academy a copy of any publication or presentation that uses the data 10 business days prior to any publication or presentation.

Process: Research Proposal must be submitted using Spectrum Academy's Institutional Review Board Research Proposal Form. Research proposals are sent directly to the Director of Academics for review. If the request is approved, an MOA is drafted and placed on the Board calendar. If it passes IRB approval, The Data Steward sends data 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

Spectrum 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, Spectrum Academy staff shall follow industry best practices outlined in the Spectrum Academy IT Security Policy for responding to the breach. Further, Spectrum 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 Spectrum Academy executive team to determine whether a security breach has occurred. If the team determines that one or more employees or contracted partners have substantially failed to comply with Spectrum 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 Director of Academics.

Spectrum Academy will provide and periodically update, in keeping with industry best practices, resources for preparing for and responding to a security breach. These resources will be made 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

Spectrum Academy Board members and staff.

7.3 POLICY

Spectrum Academy shall retain and dispose of student records in accordance with U.C.A §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 U.C.A §53A-1-1407, Spectrum Academy shall expunge student data that is stored upon request of the student if the student is at least 23 years old. Spectrum Academy may expunge medical records and behavioral test assessments, but will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. Spectrum Academy staff will collaborate with Utah State Achieves and Records Services in updating data retention schedules. 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 Spectrum Academy data governance policy is structured to encourage the effective and appropriate use of educational data. The data governance structure centers on the idea that data is the responsibility of all *S*pectrum 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, Spectrum Academy communicates data requirements and definitions to all campuses through policies and procedures.

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, Spectrum Academy provides to each of its campuses clear guidelines for data collection and the purpose of the data request. Campuses are notified as soon as possible about future data collections. Time must be given to each campus in order for them to begin gathering the data needed.

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 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

Annually, Spectrum Academy will publically post:

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

APPENDIX

Appendix A. Spectrum Academy Employee Non-Disclosure Agreement

As an employee of Spectrum 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 policies. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of Spectrum 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 Spectrum Academy's Data Security and Privacy Fundamentals Training.

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

Using _{INSERT LEA NAME HERE}_ 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 system user accounts, with staff or participating program staff.

_____I will log out of and close the browser after each use of 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 Spectrum Academy server.

Reporting & Data Sharing

_____ I will not re-disclose or share any confidential data analysis except to other authorized personnel without Spectrum Academy's expressed written consent.

_____ I will not publically publish any data without the approval of one of the Directors.

_____ 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, the only approved methods are phone calls or Spectrum Academy's Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for 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 the 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 Spectrum 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 Spectrum Academy, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of Spectrum Academy without the prior written permission of the Student Data Manager.

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 Spectrum Academy is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at school, LEA, or state-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 recoded 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 recoded to ≥99%
        2. Values of 0% to 1% are recoded 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 recoded to ≥98%
        2. Values of 0% to 2% are recoded 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 recoded to ≥95%
        2. Values of 0% to 5% are recoded 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 recoded to ≥90%
        2. Values of 0% to 10% are recoded 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 recoded to ≥80%
        2. Values of 0% to 20% are recoded 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. Example Quality Control Checklist

<u>Reliability (results are consistent)</u>

1. Same <u>definitions</u> 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. <u>Results</u> 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 Spectrum Academy data steward could reproduce the results using the information provided in the metadata

<u>Validity (results measure what are supposed to measure, data addresses the request)</u>

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

<u>Presentation</u>

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