Nebraska Department of Education Data Suppression Process Version 2.0.1

DATA SUPPRESSION PROCESS

					Document Revision Control Table			

Version No.	Date Revised	Change Description	A/M/D (Add/Modify / Deleted)	Prepared By	Approved By
1.0	3/29/2022	Initial Version	A	Bryan Helzer/ Director Data Quality & Support	Ganesan Kanagarajan/Administrator Information Systems & Services, Data Policy Committee Members (Jill Aurand, Tibor Moldovan) and Data Officer/Kristin Yates
2.0	9/6/2024	Revised	M	Bryan Helzer	Ganesan Kanagarajan/Administrator Information Systems & Services, Data Policy Committee Members (Jill Aurand, Tibor Moldovan) and Data Officer/Kristin Yates
2.0.1	2/3/2025	Revised	M	Diane Steinke	

Table of Contents

Process Responsibility Matrix

Role	R	A	C	I
Commissioner	☐	☒	☐	☐
Deputy Commissioner	☒	☐	☐	☒
Program Office Administrator	☒	☐	☐	☐
Program Specialist	☒	☐	☐	☐
Legal Counsel	☐	☐	☐	☒
External (outside NDE)	☐	☐	☐	☒
Governance Coordinator	☐	☐	☐	☒
Information Systems Officer	☐	☐	☐	☒

* (R)esponsible / (A)ccountable / (C)onsulted / (I)nformed

Introduction

Purpose:

The purpose of this Data Suppression Process document is to assist and understand compliance with privacy and confidentiality requirements under the Family Educational Rights and Privacy Act (FERPA) by reviewing basic terminology used to describe data de-identification as well as related concepts and approaches and to establish clear guidelines and procedures for identifying, handling, and suppressing sensitive or confidential information within an organization. This process serves several essential purposes:

1. **Data Privacy Compliance**: Ensures compliance with data protection regulations, such as FERPA, HIPAA, or CCPA, by outlining how sensitive data should be managed and suppressed when necessary.
2. **Protection of Personal Information**: Safeguards personal and sensitive information of educational collected data from being exposed to unauthorized individuals.
3. **Data Suppression Criteria**: Specifies the criteria and circumstances under which data should be suppressed for unauthorized disclosure of personally identifiable information from education records (PII), students' data must be adequately protected at all times.
4. **Employee Training:** Employee training and awareness programs are required to ensure staff understands and complies with the data suppression process.
5. **Monitoring and Auditing**: Describe how the organization monitors and audits data suppression practices to ensure ongoing compliance.
6. **Documentation and Record Keeping**: Mandates proper documentation of data suppression activities, including logs and records of actions taken.
7. **Continuous Improvement**: Encourages regular reviews and updates of the process to adapt to changing regulations, technologies, and business needs.

Scope:
- Data Suppression Definitions
- Data Masking Process

Out of Scope:
- Data Policy
- Data Calculations
- Privacy Policy

DATA SUPPRESSION PROCESS

Process Statement

Our organization is committed to safeguarding sensitive information through the implementation of a comprehensive data suppression process. This process outlines procedures for identifying, classifying, and securely handling data to prevent unauthorized access, disclosure, or misuse. We are dedicated to maintaining the privacy and security of our data assets in compliance with applicable regulations and standards.

Privacy of individual student records is protected under FERPA and other state and federal statutes. To avoid unauthorized disclosure of personally identifiable information from education records (PII), students' data must be adequately protected at all times. For example, when schools, districts, or states publish reports on student achievement or share students' data with external researchers, these organizations should apply disclosure avoidance strategies, to prevent unauthorized release of information about individual students. To ensure successful data protection, it is essential that techniques are appropriate for the intended purpose and that their application follows the best practices.

It is important to note that PII may include not only direct identifiers, such as names, student IDs or social security numbers, but also any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification. Therefore, simple removal of direct identifiers from the data to be released does not constitute adequate de-identification. Properly performed de-identification involves removing or obscuring all identifiable information until all data that can lead to individual identification have been expunged or masked. Further, when deciding as to whether the data have been sufficiently de-identified, it is necessary to take into consideration cumulative re-identification risk from all previous data releases and other reasonably available information, including publicly available directory information and de-identified data releases from education records as well as other sources.

Data Suppression Definitions

De-identification [of data] refers to the process of removing or obscuring any personally identifiable information from student records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them. Specific steps and methods used to de-identify information (see disclosure limitation method for details) may vary depending on the circumstances but should be appropriate to protect the confidentiality of the individuals. While it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify an individual. De-identified data may be shared without the consent required by FERPA (34 CFR §99.30) with any party for any purpose, including parents, general public, and researchers (34 CFR §99.31(b)(1)). These data are typically released in the form of aggregated data (such as tables showing numbers of enrolled students by race, age, and sex) or microdata (such as individual-level student assessment results by grade and school). Please see the Reporting section on pages 12-15 for examples.

Disclosure limitation method (also known as **disclosure avoidance method**) is a general term referring to a statistical technique used to manipulate the data prior to release to minimize the risk of inadvertent or unauthorized disclosure of PII. Entities releasing data should apply a consistent de-identification strategy to all of their data releases of a similar type (e.g., tabular and individual level data) and similar sensitivity level. It is advised that organizations document their data reporting rules in the documents describing their data reporting policies and privacy protection practices, such as a Data Governance Manual. (See PTAC's Data Governance and Stewardship brief at https://studentprivacy.ed.gov/resources/issue-brief-data-governance-and-stewardship for more information on best practices in data governance.) The major methods used by the U.S. Department of Education for disclosure avoidance for tabular data include defining a minimum cell size (meaning no results will be released for any cell of a table with a number smaller than "X" or else cells are aggregated until no cells based on one or two cases remain) and controlled rounding (meaning that cells with a number smaller than "X" require that numbers in the affected rows and columns be rounded so that the totals remain unchanged). Whenever possible, data about individual students (e.g., proficiency scores) are combined with data from a sufficient number of other students to disguise the attributes of a single student. When this is not possible, data about small numbers of students are suppressed.

Masking is a disclosure limitation method that is used to "mask" the original values in a data set to achieve data privacy protection. This general approach uses various techniques, such as data perturbation, to replace sensitive information with realistic but inauthentic data or modifies original data values based on pre-determined masking rules (e.g., by applying a transformation algorithm). The purpose of this technique is to retain the structure and functional usability of the data, while concealing information that could lead to the identification, either directly or indirectly, of an individual student. Masked data are used to protect individual privacy in public reports and can serve as a useful alternative for occasions when the real data are not required, such as user training or software demonstration. Specific masking rules may vary depending on the sensitivity level of the data and organizational data disclosure policies.

DATA SUPPRESSION PROCESS

Suppression is a disclosure limitation method which involves removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This method may often result in very little data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of PII (e.g., complementary suppression of one or more non-sensitive cells in a table so that the values of the suppressed cells may not be calculated by subtracting the reported values from the row and column totals). Correct application of this technique generally ensures low risk of disclosure; however, it can be difficult to perform properly because of the necessary calculations (especially for large multi-dimensional tables). Further, if additional data are available elsewhere (e.g., total student counts are reported), the suppressed data may be re-calculated.

FERPA requires personally identifiable information to be de-identified whenever there is public reporting of personally identifiable information from an education record including: race/ethnicity, gender, poverty (eligible for free and reduced lunch program), eligibility or participation in Special Education or other programs, student achievement, and assessment data. According to the FERPA guidance, masking of data must be sufficient so that it is not possible for a "reasonable person in the school community who does not have personal knowledge of the relevant circumstances" to identify individual students based on reasonably available information, including other public information released by the agency, such as a report presenting detailed data in tables with small size cells (34 CFR 99.3 and 99.31(b)(1)).

DATA SUPPRESSION PROCESS

Primary Suppression Rules

- Rule of 10 – Used to protect personally identifiable information when the number of students in a group is small. Nebraska masks all numbers when there are fewer than 10 in a group. Membership is not masked at the State, district, school and grade level even if fewer than 10 students.

- Performance Level Reporting – When reporting student performance on assessments in levels
  - The percentages are displayed when there are 5 or more at a performance level.
  - All data are still masked for groups of fewer than 10.

- Rule of 100% – Used to protect privacy in student performance when all students in a group fall into the same achievement level regardless of the total student count; these values will be suppressed.

Secondary Suppression Rules

- Complementary Suppression – If any cell less than the N-Size (10, or 5 for Performance Levels) and only one value is suppressed in a row or column, the next highest value in that row or column is also suppressed. If there are multiple occurrences of this value, one occurrence will be randomly suppressed.

- Total Values – Totals are retained whenever possible by implementing complementary suppression at the row/column level.

- Zero Values
  - Fields with a value of 0 are suppressed where, if a percentage is calculated, the numerator is zero, but the denominator is greater than 0.
  - If the denominator would be zero, there should be an indicator to show that no students were in the group.
  - For public reporting on the Nebraska Education Profile (NEP), all categories by which data are parsed (e.g., race, EL) are presented in the report table even if there are no data for categories. The one exception to this is the Student Discipline report.[i]

Reporting

Primary Suppression Rules

Consider the following set of Performance Data

Group	Students Tested	Developing	Developing Percent	On Track	On Track Percent	College & Career Ready	College & Career Ready Percent
All Students	281	181	64.41%	77	27.40%	23	8.19%
Highly Mobile	5	4	80.00%	1	20.00%	0	0.00%
Homeless	4	4	100.00%	0	0.00%	0	0.00%
Military Family	0	0	0.00%	0	0.00%	0	0.00%
RACE ETHNICITY							
American Indian or Alaska Native	11	9	81.82%	1	9.09%	1	9.09%
Asian	11	3	27.27%	7	63.64%	1	9.09%
Black or African American	13	5	38.46%	5	38.46%	3	23.08%
Hispanic	193	135	69.95%	48	24.87%	10	5.18%
Two Or More Races	11	4	36.36%	5	45.45%	2	18.18%
Native Hawaiian or Other Pacific Islander	3	3	100.00%	0	0.00%	0	0.00%
White	39	22	56.41%	11	28.21%	6	15.38%
SPECIAL EDUCATION							
Children Without Disabilities	247	157	63.56%	70	28.34%	20	8.10%
Children with Disabilities	34	24	70.59%	7	20.59%	3	8.82%

DATA SUPPRESSION PROCESS

The following Primary Suppression rules are then implemented:
- Rule of 10
- Performance Level Reporting Rule of 5

Group	Students Tested	Developing	Developing Percent	On Track	On Track Percent	College & Career Ready	College & Career Ready Percent
All Students	281	181	64.41%	77	27.40%	23	8.19%
Highly Mobile	*	*	*	*	*	*	*
Homeless	*	*	*	*	*	*	*
Military Family	0	0	0.00%	0	0.00%	0	0.00%
RACE ETHNICITY							
American Indian or Alaska Native	11	9	81.82%	*	*	*	*
Asian	11	*	*	7	63.64%	*	*
Black or African American	13	5	38.46%	5	38.46%	*	*
Hispanic	193	135	69.95%	48	24.87%	10	5.18%
Two Or More Races	11	*	*	5	45.45%	*	*
Native Hawaiian or Other Pacific Islander	*	*	*	*	*	*	*
White	39	22	56.41%	11	28.21%	6	15.38%
SPECIAL EDUCATION							
Children Without Disabilities	247	157	63.56%	70	28.34%	20	8.10%
Children with Disabilities	34	24	70.59%	7	20.59%	*	*

Complementary Suppression Rules

As you can see, the data set with Primary Suppression allows for derivation of data.

- The only Race Ethnicity suppressed due to the Rule of 10 is Native Hawaiian and Other Pacific Islander. This means that the number of Students Tested can be derived. The next lowest count of Students Tested is Asian, so the count of Students Tested will be suppressed.

- For the Black or African American Race Ethnicity, we know that 13 students were tested, 5 were Developing and 6 were On Track. It can then be derived that 2 students were College & Career Ready, even though those numbers are suppressed. Complementary suppression will be implemented on the next lowest Performance Level, which is Developing.

- For Children with Disabilities, we know that 35 students were tested, 23 were Developing, 10 were On Track, and 2 were College & Career Ready. Complementary suppression will be implemented on the next lowest Performance Level, which is On Track. HOWEVER, this is still not sufficient, as we are required to publish this information for the number of Children Without Disabilities. Because the On Track and College & Career Ready Performance Levels are suppressed for Children with Disabilities, we will need to suppress these same Performance Levels for the Children without Disabilities.

DATA SUPPRESSION PROCESS

The data now displays as:

Group	Students Tested	Developing	Developing Percent	On Track	On Track Percent	College & Career Ready	College & Career Ready Percent
All Students	282	180	63.83%	80	28.37%	22	7.80%
Highly Mobile	*	*	*	*	*	*	*
Homeless	*	*	*	*	*	*	*
Military Family	0	0	0.00%	0	0.00%	0	0.00%
RACE ETHNICITY							
American Indian or Alaska Native	12	8	66.67%	*	*	*	*
Asian	*	*	*	7	63.64%	*	*
Black or African American	13	*	*	6	46.15%	*	*
Hispanic	193	135	69.95%	48	24.87%	10	5.18%
Two Or More Races	11	*	*	5	45.45%	*	*
Native Hawaiian or Other Pacific Islander	*	*	*	*	*	*	*
White	39	22	56.41%	11	28.21%	6	15.38%
SPECIAL EDUCATION							
Children Without Disabilities	247	157	63.56%	*	*	*	*
Children with Disabilities	35	23	65.71%	*	*	*	*

Additional Suppression Rules for Proficiency

- Percent Proficient is calculated by combining students with performance levels of On Track and Advanced. In order to preserve Percent Proficient whenever possible, when Primary Suppression results in only one performance level being suppressed, and if that performance level is either On Track or Advanced, we will implement Complementary Suppression on the other (On Track or Advanced) performance level. This will allow us to display Percent Proficient.

- Because Developing is the only performance level used to calculate Percent Below Proficient, if Developing has to be masked, Percent Proficient must also be masked. The reverse is also true; if Percent Proficient has to be masked, then Developing must be masked.

Exceptions to Suppression

- Membership data is not masked. This includes membership in total and by race/ethnicity.

Glossary of Terms

Complementary: A method of data masking that combines multiple similar/related groups within the same dataset obscuring specific results of an individual, such as combining results of American Indian or Alaska Native (AM) and Native Hawaiian or Other Pacific Islander (PI) instead of individually.

Data Masking: Also known as data obfuscation, hides the actual data using modified content like characters or numbers. The main objective of data masking is creating an alternate version of data that cannot be easily identifiable or reverse engineered, protecting data classified as sensitive.

Data Suppression: A disclosure limitation method that involves removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This is often represented as an asterisk "*".

PII: Personally identifiable information - any information that can be used to uniquely identify an individual directly or indirectly, such as a name, home address, email address, or IP address.

Non-PII: Non-Personally identifiable information – any information about an individual that by itself would be difficult to identify an individual, such as postal code, gender, age, or race.

SPII: Sensitive Personally identifiable information - any PII that if lost, stolen, or disclosed without authorization could result in significant harm to an individual, such as social Security number, Alien registration number, driver's license, or state identification number.

Linkable Information: any combination of information that can be used to increase the ability to identify an individual directly or indirectly. This also changes the information, such as combination of non-PII can become PII or SPII, as well as other combinations specific information can change to other information types.

PHI: Protected health information - specific type of SPII that is collected by a healthcare provider or other covered entity for the provision of healthcare services, such as allergies, medications, biometrics, medical history, and conditions.

PCI-DSS: Payment card information

ITAR: Intellectual property

SDM: Static data masking – a method of applying data masking by permanently replacing sensitive data by altering data at rest, such as creating a copy of production data and applying data masking.

DDM: Dynamic data masking – a method of replacing sensitive data in transit leaving the original at-rest data intact and unaltered, such as using a proxy to determine and alter the data depending on the requestor's role.

Encryption: A method of data masking that requires a key to be able to decrypt information which is otherwise unreadable.

Scrambling: A method of data masking that jumbles characters in random order.

Nulling: A method of data masking that completely suppresses the data value.

Substitution: A method of data masking that replaces values with random pseudo-values.

Shuffling: A method of data masking that uses actual data but is randomly mixed so an individual cannot be determined.

Variance: A method of data masking by applying

References

- [Handbook for safeguarding Sensitive PII](#) - Homeland Security
- https://cdn.education.ne.gov/wp-content/uploads/2017/07/Nebraska_Data_Access_and_Use_Policy_and_Procedures.pdf - NDE Data Access and Use Policy
- https://studentprivacy.ed.gov/ - Federal regulations resources, U.S. Department of Education
- https://studentprivacy.ed.gov/ferpa - FERPA | ed.gov
- https://www.fns.usda.gov/cn/disclosure-requirements-child-nutrition-programs - Disclosure Requirements for the Child Nutrition Programs
- https://nces.ed.gov/pubs2004/privacy/section_2b.asp - Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies - 2.B. Privacy Protection Under FERPA: Responsibilities of Agencies and Schools
- https://slds.ed.gov/#program – SLDS Technical Assistance Program Website
- https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf - Data De-identification: An Overview of Basic Terms

---

[i] Aurand, Jill: February 3, 2025.