# The Nevada Department of Education

# Security and Privacy Policy Information


Version: [12/2021]

# The Nevada Department of Education Data Access and Use Policy (DAUP)

## Overview

NDE values the use of data to improve student achievement and system performance while recognizing the importance of ensuring data are accessed and used appropriately. This section outlines the federal and State statutes and regulations associated with educational data privacy, along with NDE policies and procedures related to educational data security and privacy, including data collection, data access, data disclosure, data sharing agreements, and data requests. These policies and procedures allow NDE to provide accurate and timely data to stakeholders, while securely protecting student data in accordance with relevant laws and regulations.

## Federal and State Statute, Regulations, and Policies Related to Data Security

The primary federal law that protects student privacy is the Family Educational Rights and Privacy Act (FERPA), housed within 20 U.S. Code (USC) §1232a, along with associated regulations in the Code of Federal Regulations (CFR) (34 CFR §99). FERPA provides parameters around the sharing of student information. The State considers FERPA the policy floor, not the ceiling; therefore, the State has implemented policies and procedures above and beyond FERPA to manage and protect the privacy of student data.

Various Nevada State laws and policies are also linked to student data privacy:

- NRS 288.267 requires NDE to adopt policies and procedures consistent with State and federal laws related to the privacy of student data,
- NRS 388.272 outlines provisions that must be included in NDE contracts involving personally identifiable information (PII, see Disclosure of PII for a definition); and
- NRS 388.273 requires NDE to adopt a plan that provides for the security of any data concerning pupils that is collected, maintained, and transferred by the Department.

The main State policy for general data security is the Consolidated State Information Security Policy (SISP), developed by the Nevada Department of Enterprise Information Technology Systems (EITS) Office of Information Security (OIS). NDE follows these standards and is a member of the State Security Policy Committee. The State Information Security Policy was developed based on the International Standard Code of Practice for Information Security Management (ISO/IEC 27002:2005) and the National Institute of Standards and Technology (NIST) Special Publication 800-series. Compliance with the SISP is mandatory for all state agencies with the exception of the Nevada System of Higher Education (NSHE) and the Nevada Criminal Justice Information Computer System. In cases where entities cannot comply with any section of the SISP, an exception request must be documented and all potential risks must be identified and submitted to the OIS for approval. See the SISP for more detailed information and Appendix A for relevant federal and state statute and regulations.

# Data Collection

## Overview

The NDE adheres to federal and State statutes and regulations governing data policy and reporting requirements, including those related to: student, educator, school, and district performance; evaluation of educational programs; and allocation of state funding. To meet these obligations, NDE must collect myriad data related to students, educators, schools, programs, and school districts.

## When the NDE Collects Data

Data are collected by NDE only when necessary; collections are limited to the specific policy needs outlined above. Data collections are ongoing throughout the year and often driven by program-specific timelines and deadlines.

## Data NDE Collects

NDE collects a range of data that meet specific policy, practice, and service needs. Some data are subject to privacy laws and regulations, such as student-level data that contains personally identifiable information (PII, see Disclosure of PII for a definition). Other data are not subject to privacy laws and regulations, such as school names or fiscal data. Per NRS 388.268, NDE maintains a data dictionary that lists many student-level data elements collected and maintained by NDE. The dictionary itself does not contain data. Additional student-level data elements are collected in the State student information system; these data are a subset of the data collected in the local student information systems. Both the State and local student information systems are currently on the Infinite Campus platform.

## How the NDE Collects Data

In accordance with relevant laws and regulations, NDE uses various methods to securely collect data. NDE maintains a secure file transfer portal that is used whenever data containing PII are collected or shared. Data containing PII should **never** be transferred via email. NDE also uses various data collection applications that allow entities to securely submit data to NDE. Any data collected and stored by NDE is at all times under the control of NDE. See the Secure Methods of Transmitting Data Electronically section for more information.

# Access to/Disclosure of Data

## Overview

Under FERPA, NDE may not allow access to (disclose) PII from educational records by any third party, unless written consent has been provided by the parent, legal guardian, or eligible student (34 CFR §99.30), except in certain circumstances (34 CFR §99.31) outlined the Disclosure of PII section. NDE is required to use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses PII (34 CFR §99.31(c)). Per 34 CFR §99.31(d), NDE maintains the discretion to disclose PII, except to parents, legal guardians, or eligible students. In accordance with these requirements, NDE only allows direct access to data containing PII to department personnel and contracted entities.

## Access to Data by NDE Staff and Authorized Agents

FERPA allows State and local educational authorities to access student PII (34 CFR §99.31(a)(3)). However, the data containing PII that NDE collects and stores are only available to staff and authorized agents who (1) have undergone a background check and (2) have a legitimate need for data access, such as those that perform duties involving evaluation, audit, compliance tasks, etc. NDE's Data Governance Board ensures access to PII is limited to appropriate staff by processing internal data requests (see the Internal Data Requests section). The Board also annually provides NDE Leadership with a list of authorized representatives within NDE with access to PII.

## Access to Data by Parents, Legal Guardians, and Eligible Students

FERPA gives custodial and noncustodial parents alike certain rights with respect to their student's education records (34 CFR §99.10 *et seq.*), unless the agency or institution has been provided with evidence that there is a court order, state statute, or legally binding document relating to such matters as divorce, separation, or custody that specifically revokes these rights (34 CFR §99.4). Otherwise, both custodial and noncustodial parents have the right to access their student's education records (34 CFR §99.10), the right to seek to have the records amended (34 CFR §99.20), the right to consent to disclosure of PII from the records (except in certain circumstances) (34 CFR §99.30 and §99.31), and the right to file a complaint with NDE (34 CFR §99.63). When a student reaches 18 years of age or attends a postsecondary institution, they become an "eligible student," and all rights under FERPA transfer from the parent to the student (34 CFR §99.5). NDE must comply with a parent or legal guardian's request to review educational records within a reasonable timeframe, but not more than 45 days after receiving such a request (34 CFR §99.10). NDE may provide the educational records directly to the parent or legal guardian, to the local school district for review, or by making other appropriate arrangements. Per Code of Federal Regulations (34 CFR §99.11), unless the imposition of a fee effectively prevents a parent or eligible student from exercising the right to inspect and review the student's education records, an educational agency or institution may charge a fee for a copy of an education record which is made for the parent or eligible student. An educational agency or institution may not charge a fee to search for or to retrieve the education records of a student. NDE may ask for legal certification denoting parenthood (such as a birth certificate) or guardianship, as well as other forms of identification if needed. Alternatively, NDE may work with the local school district or school to verify the requestor's identity and status as the student's parent or legal guardian.

## Access to Data by School Officials

FERPA allows "school officials" within a school/district to obtain access to PII provided the agency or institution has determined that they have "legitimate educational interest" in the information (34 CFR §99.31(a)(1)). According to the U.S. Department of Education, the term "school official" is generally interpreted as: district and school administrators; educational personnel; health staff; counselors; attorneys; clerical staff; trustees; members of committees and disciplinary boards; and a contractor, volunteer or other party to whom the school has outsourced institutional services or functions. NDE is required to use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests (34 CFR §99.31(c)). A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or

functions may also be considered a "school official" provided certain criteria are met (34 CFR §99.31(a)(1)(i)(B)).

## Access to Data by External Entities

In accordance with FERPA, NDE does not disclose PII to or allow access to data containing PII by external entities, except in certain circumstances (see the Disclosure of PII section for more information).

## Types of Data Disclosure

To comply with federal and State laws and regulations, NDE must frequently disclose data. In some cases, NDE discloses data in aggregate or de-identified form, while in others, PII is disclosed. Disclosure of PII can be authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party (e.g., a researcher). Disclosure of PII can also be unauthorized or accidental. An unauthorized disclosure can happen due to a data breach. NDE also maintains educator data, which can sometimes be shared. Each of these types of disclosure is further outlined below.

### *Disclosure of Aggregate Student Data*

Aggregate data refers to numerical or non-numerical information that is (1) collected from multiple sources and/or on multiple measures, variables, or individuals and (2) compiled into data summaries or summary reports, typically for the purposes of public reporting. When disclosing aggregate data, there is still a need to protect PII. The aggregation of student-level data removes much of the risk of disclosure, since no direct identifiers (e.g. name, student ID, etc.) are present in the aggregated tables. However, some risk of disclosure does remain where one or more students possess a unique or uncommon characteristic(s) that would allow them to be identified in the data table. In these cases, some level of action (termed "disclosure avoidance") is necessary to prevent disclosure of PII in the aggregate data table(s). In these situations, NDE utilizes various disclosure avoidance techniques, which are further outlined in the Data Disclosure Avoidance Rules section.

### *Disclosure of De-Identified Student Data*

De-identified data are data from which all PII has been removed or modified to protect individual identities and privacy. Per 34 CFR §99.31(b), NDE may release records or information after the removal of all PII provided that NDE has made a reasonable determination that students are not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. See the Data Request section for more information on how NDE may disclose de-identified student-level data through the data request process.

### *Disclosure of PII*

PII includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. FERPA regulations (34 CFR §99.3) define PII as a term that includes, but is not limited to:

a) The student's name;
b) The name of the student's parent or other family members;
c) The address of the student or student's family;

d) A personal identifier, such as the student's social security number, student number, or biometric record;
e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

In compliance with federal and state laws and regulations, NDE does not disclose PII from student records unless the disclosure is for one of the limited purposes outlined in 34 CFR §99.31.

Per 34 CFR §99.31, NDE may disclose PII for:

a) Use by school officials for legitimate educational purposes (see 34 CFR §99.31(a)(1)). PII may be disclosed to school officials if the official needs to review an educational record in order to fulfill their professional responsibility. See the Access to Data by School Officials section for more information on school officials.
b) Student transfer and enrollment (see 34 CFR §99.31(a)(2)). Student information may be disclosed to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled, so long as the disclosure is for purposes related to the student's enrollment or transfer.
c) Use by authorized representatives (see 34 CFR §99.31(a)(3)), including:
    - The U.S. Comptroller General;
    - The U.S. Attorney General;
    - The U.S. Secretary of Education; or
    - State and local educational authorities.
d) Educational studies (see 20 USC §1232g(b)(1)(F) and 34 CFR §99.31(a)(6)). PII may be disclosed to organizations conducting studies for, or on behalf of, NDE to: (1) develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction. Studies must ensure:
    - The study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information;
    - The information is destroyed when no longer needed for the purposes for which the study was conducted; and
    - There is a written agreement that meets the requirements outlined in the Data Sharing section of this document.
e) Evaluation/audit or compliance activities (see 20 USC. 1232g(b)(1)(C), (b)(3), and (b)(5) and 34 CFR §99.31(a)(3) and §99.35). Student information may be disclosed to authorized representatives of the NDE in connection with an audit or evaluation of federal- or State-supported education programs, or for the enforcement of or compliance with federal legal

requirements that relate to those programs. Disclosure for the purposes of such audits, evaluations, or compliance activities must ensure that the NDE uses reasonable methods to ensure that its authorized representative:

- Uses PII only to carry out an audit or evaluation of federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs;
- Protects the PII from further disclosures or other uses, as specified in 34 CFR §99.35.
- Destroys the PII in accordance with 34 CFR §99.35(b) and 34 CFR §99.35(c); and
- Enters into a written agreement with the NDE that meets the requirements outlined in the Data Sharing section of this document.

f) Compliance with a judicial order or lawfully issued subpoena (see 34 CFR §99.31(a)(9)).
g) Use in a health and safety emergency (see 34 CFR §99.31(a)(10) and §99.36).
h) Use by parents of a student who is not an eligible student or to the eligible student (see 34 CFR §99.31(a)(12)). In these cases NDE does not have discretion over disclosure and is required to disclose records. See the Access to Data by Parents, Legal Guardians, and Eligible Students section for more information.

### *Disclosure of Educator Data*

NDE is responsible for several activities that require the collection of data for educators in Nevada. As the entity responsible for issuing and renewing educator licenses, linking student achievement to practicing educators, and monitoring implementation of local educator evaluation systems, NDE must manage and secure information that is sensitive and confidential. NDE maintains several statutory and regulatory protections to keep educator data private.

Except as otherwise provided in NRS 239.0115, files relating to the application, including the applicant's health records, fingerprints and any report from the Federal Bureau of Investigation or the Central Repository for Nevada Records of Criminal History, transcripts, scores on examinations as required by the Commission, correspondence concerning the application, and any other personal information (personal information is defined in NRS 603A.040) are classified as confidential (confidentiality of application is defined in NRS 391.035). Each educator has the right to inspect and to have copies made (at the educator's expense) of all information pertaining to the educator. The educator information may be disclosed in the normal and proper course of administering licenses and authorizations, but it is otherwise unlawful for any NDE employee or other person to divulge, or make known in any way, any such personal information without the written consent of the educator. Personnel information may be disclosed in the aggregate, so long as the identities of individual educators remain anonymous and the data pool is large enough to prevent the identification of individual educators, which in no instance shall be smaller than ten (10) educators.

NRS 385A.800 clarifies that, while NDE may collect information concerning an individual educator and student assessment results linked to that educator/classroom in order to fulfill duties as required by law, this information may, at NDE's discretion, be shared so long as the confidentiality of each individual pupil is protected.

Through NDE's website, there is a public page for **Educator Licensure Lookup**. License information on the site reflects information in the NDE database; however, applications and forms are subject to standard processing time, and the information here does not reflect pending changes which are being reviewed.

# Data Sharing Agreements

## Overview

FERPA generally does not allow disclosure of PII without written consent. However, FERPA includes exceptions that permit data sharing under specified conditions with agencies, vendors, or individuals to conduct studies, audit or evaluate programs, or enforce/comply with legal requirements (see 34 CFR §99.31(a)(6), §99.35, and the Disclosure of PII section for more information). FERPA also allows data sharing with contractors, volunteers, or other individuals performing services for the educational institution under certain circumstances.

In these situations, written data sharing agreements must be used to protect student data. A data sharing agreement is a formal contract that details topics such as what data are being shared and how the data can be used. A data sharing agreement protects NDE by ensuring that the data will not be misused, and also prevents miscommunication between NDE and the receiver. Requirements for data sharing agreements can differ depending on the conditions and parties involved.

Prior to sharing PII for studies conducted on behalf of the NDE or for audits, evaluation, or compliance monitoring, NDE is required by FERPA (see 34 CFR §99.31(a)(6)(iii)(C) and §99.35) to enter into a written agreement that meets certain requirements. NDE has added criteria beyond the FERPA requirements. The written agreement must:

1. Designate the individual that will serve as the authorized representative responsible for managing the data in question.
2. Specify the purpose, scope, and duration of the study/studies and the information to be disclosed.
3. Require the authorized representative to use PII from education records only to meet the purpose(s) of the study as stated in the written agreement.
4. Require the authorized representative to conduct the study in a manner that does not permit personal identification of parents and students by anyone other than representatives of the organization with legitimate interests.
5. Require the authorized representative to destroy all PII when the information is no longer needed for the purposes for which the study was conducted and specifies the time period in which the information must be destroyed. The parties to the written agreement may agree to amend the agreement to extend the time period if needed.
6. Ensure appropriate technical, physical, and administrative safeguards to protect PII at rest and in transit. Examples of this include secure-file transfer protocols (SFTP) and hyper-text transfer protocol over secure socket layer (HTTPS).

7. Include a requirement that any breach in security must be reported immediately to the authorized representative of NDE.

NRS 388.272 also requires contracts entered into by NDE that provide for the disclosure of student PII to include (1) provisions specifically to protect the privacy and security of the PII and (2) a penalty for intentional or grossly negligent noncompliance with the terms of the contract, including, without limitation, provisions for termination of the contract and for the payment of monetary damages for any breach of the terms of the contract.

## Monitoring Implementation of Data Sharing Agreements

In addition to all of the precautions addressed above, any NDE data sharing agreement or contract may also include the following assurances to protect PII from further disclosure and unauthorized use:

- That NDE may verify that the authorized representative has a data stewardship plan that details the organization's data privacy/security policies and procedures, including the ongoing management of data collection, processing, storage, maintenance, use, and destruction. NDE may also verify that the authorized representative has a training program for its employees related to FERPA and the protection of PII.
- That NDE will maintain the right to conduct audits or other monitoring activities of the authorized representative's policies, procedures, and systems.
- That NDE will maintain the right to (1) review any data prior to publication, (2) verify that proper disclosure avoidance techniques have been used, and (3) approve reports prior to publication to ensure they reflect the original intent of the agreement.

## Failures to Comply with Data Sharing Agreements

Written complaints may be filed with NDE regarding an alleged violation of a data sharing agreement or contract. A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. NDE will investigate all reasonable complaints following the procedure outlined under the Data Breaches section of this document. NDE, in collaboration with the EITS Office of Information Security, may also conduct its own investigation if a complaint has not been filed or a complaint has been withdrawn to determine whether a violation has occurred.

As required by FERPA, if an authorized representative improperly rediscloses PII, NDE shall deny that representative further access to PII for at least five years (34 CFR §99.67). In addition, NRS 388.272 requires NDE contracts to include provisions for a penalty for intentional or grossly negligent noncompliance with the terms of the contract, including, without limitation, provisions for termination of the contract and for the payment of monetary damages for any breach of the terms of the contract.

Furthermore, NDE may pursue penalties permitted under state contract law (NRS603A.040 and NRS 333.365), such as liquidated damages.

# Data Request Management

## Overview

NDE acknowledges that internal and external education stakeholders—including students, parents, teachers, school administrators, taxpayers, business leaders, and policymakers—need data to support student learning. NDE strives to make information available to the public on various reporting platforms and websites such as the Nevada Report Card, Nevada School Performance Framework (NSPF), the NDE website, etc. If data are not publicly available and are needed for a study or research by an individual or entity, then an official data request must be submitted. This section outlines how NDE manages data requests.

## Data Request Process

An NDE Data Request Form must be submitted for any type of data request, including those that do or do not involve PII. All data requests must be accompanied by a data request form, including data requested by NDE staff. NDE maintains a log of data requests, which the NDE Data Governance Board reviews and approves/denies at their monthly meetings.

If a request is approved, data disclosure avoidance techniques will be applied to the data as needed. As a general rule, data requests for PII will be denied, unless the request falls under one the FERPA exceptions for (1) organizations conducting studies on behalf of NDE and (2) audit, evaluation, and compliance monitoring (see the Disclosure of PII section for more information). In those cases, NDE will require a Data Sharing Agreement prior to fulfilling the data request.

## Types of Data Requests

### *High-Priority Data Requests*

High-priority data requests always receive precedence over any other type of data request. Only data requests from the following entities are considered high priority:

- NDE Superintendent of Public Instruction, Deputy Superintendents, and members of the Superintendent's Cabinet (Chief Strategy Officer, Public Information Officer, and Management Analyst)
- The Nevada Governor's Office
- The Nevada Legislative Counsel Bureau (LCB)

### *Internal Data Requests*

Internal data requests are those from:

- NDE staff
- NDE contractors/vendors
- State of Nevada agencies
- The Nevada System of Higher Education (NSHE)

- Media/Press/Reporters (if submitted through the NDE Public Information Officer)

### *External Data Requests*

External data requests are those from individuals or organizations who are:

- Not affiliated with an agency of the State of Nevada
- Not affiliated with NSHE
- Not an NDE contractor/vendor

The Board considers external data requests on a case-by-case basis. Decisions are based on many factors including alignment of the purpose of the request with NDE's mission and the Department's capacity to fulfill the request, including constraints due to resources. A fully executed data sharing agreement is required for requests that include PII. The Board will review each external data request to determine if the request can be fulfilled based on the information provided in the request. Any external request for student-level data containing PII will go through additional layers of review and, if approved, will require a data sharing agreement to be signed in order to fully protect the data. In such cases, NDE staff will schedule and coordinate the production and secure transmission of the data to the approved requestor.

External data requesters must meet all of the Board criteria prior to obtaining access to any student-level data from NDE. One of these criteria is that the researchers have completed training on the ethical and professional standards for protecting human research participants. Potential users such as doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies must submit proposals before receiving data and conducting and publishing their research. The Board considers and reviews all requests to conduct research using Nevada student or school system data that will require additional data collection (i.e., not already collected by NDE). In the event of such a request, the Board will determine the feasibility of such a collection and forward the request with an analysis and recommendation to the Superintendent for review and approval or denial of such a request.

# Data Protocols

## Data Storage

The information security policies, standards, and procedures adopted by the State of Nevada define the principles and terms of the Information Security Program for the Executive Branch of the Nevada State Government and establish the baseline for agencies' information security programs. NDE's data storage procedures are defined by these principles and terms. More information about the baselines can be found here.

## Data Retention

Data retention schedules establish guidelines regarding the length of time records must remain accessible for future use or reference, as well as when and how the record can be destroyed when it is no longer needed. Retention schedules are determined by the record type and the business, legal and compliance requirements associated with the record.

NDE follows the records retention schedules issued by the Records Management Program within the Archives and Public Records unit at the Nevada State Library. If a record does not have a retention schedule it is kept indefinitely.

## Staff Training

All NDE employees must sign and adhere to NDE's Acceptable Use Policy, which describes the permissible uses of State technology and information, and participate in the security awareness training provided by the state. All NDE employees must also sign and adhere to the NDE Employee Data Sharing and Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data.

To minimize the risk of human error and misuse of information, NDE provides a range of training opportunities for staff that adheres to the State Information Security Program. NDE employees are required to participate in an annual information security and privacy training. NDE requires additional information security training for specific groups within the agency such as system administrators and other technical personnel. NDE also provides guidance to school districts concerning compliance with state and federal privacy laws and best practices.

## Data Breaches

Any data breach or concerns regarding a data breach must be reported immediately to NDE's director of Information Technology. If the director, in collaboration with NDE's Information Security Officer (ISO), determines that one or more employees or contracted partners have substantially failed to comply with NDE's information security and privacy policies, they will report the incident to the Deputy Superintendent of the relevant Division, the Superintendent, and Nevada's Office of Information Security (OIS). Consequences for a breach may include termination of employment and further legal action. Concerns about breaches that involve the Director of Information Technology must be reported immediately to the ISO and Superintendent of Public Instruction. The Superintendent and the ISO will collaborate with the EITS Office of Information Security to determine whether a security breach has

occurred and will identify appropriate consequences, which may include termination of employment or a contract.

## Data Breach Incident Response Team

The Department is responsible for developing and maintaining a Data Breach Incident Response Team. The standing team is comprised of the Director of Information Technology, the Information Security Officer, the Superintendent of Public Instruction, the Chief Strategy Officer, and the Public Information Officer. Depending on the nature of the incident, the affected program data stewards may join the response team. Upon the occurrence of a data breach, a Team Manager should be established to conduct the business of the Incident Response Team and a back-up should be identified should the Manager be unavailable. Once it has been determined a data breach has occurred, or information regarding a potential data breach has been identified and reported to the Superintendent of Public Instruction, the Incident Response Team will assemble and assume the role of directing the mitigation efforts of the Department.

## Data Breach Communication Guidelines

All communications regarding a data breach or potential data breach will be handled through the Incident Response Team. No other individual within the Department should communicate any information regarding a data breach or potential breach to anyone except members of the Incident Response Team.

*Media:* The incident handling team should establish media communications procedures that comply with the organization's policies on media interaction and information disclosure. For discussing incidents with the media, NDE relies on the Public Information Officer, with the Chief Strategy Officer serving as a backup contact. The designated contacts should be considered prepared for communicating with the media regarding data breach incidents as follows:

- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information, such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Remind all staff of the general procedures for handling media inquiries.
- Hold mock interviews and press conferences during incident handling exercises. The following are examples of questions to ask the media contact:
    - Who attacked you? Why?
    - When did it happen? How did it happen? Did this happen because you have poor security practices?
    - How widespread is this incident? What steps are you taking to determine what happened and to prevent future occurrences?

- What is the impact of this incident? Was any personally identifiable information (PII) exposed? What is the estimated cost of this incident?

*Law enforcement:* The Incident Response Team will work directly with the Deputy Attorney General assigned to support NDE to discuss conditions under which incidents should be reported to law enforcement, how the reporting should be performed, what evidence should be collected, and how it should be collected. Law enforcement may only be contacted by individuals designated by the Superintendent or a Deputy Attorney General. The designee(s) should be familiar with the reporting procedures for all relevant law enforcement agencies and well prepared to recommend which agency, if any, should be contacted. The Incident Response Team should understand what the potential jurisdictional issues are (e.g., physical location—an organization based in one state has a server located in a second state attacked from a system in a third state, being used remotely by an attacker in a fourth state).

## Data Disclosure Avoidance Rules

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each individual's personally identifiable information (PII). 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 NDE and local school districts is comprehensive, the data made available to the public is redacted, i.e. suppressed, to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state level reports.

### When does NDE redact data?

NDE redacts any data/information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Examples of the data that is connected to student educational outcomes are such as but not limited to assessment results, graduation rates, dropout rates, retention rates, special population membership status and more. See examples under the section “What methods does NDE use?” about suppression and top and bottom coding.

### Exception to Applying Disclosure Avoidance Techniques

The only exception to applying disclosure avoidance techniques is to basic entity level enrollment counts (for example October student counts), including total enrollment and those broken down by race/ethnicity and gender. Besides this exception, under FERPA and other applicable federal and State privacy statutes and regulations, when publicly reporting or fulfilling data requests NDE applies disclosure avoidance techniques to any student counts or percentages relating to student enrollment, characteristics, performance, outcomes, etc.

## What methods does NDE use?

NDE has implemented a system that not only suppresses *n* size of greater than 0 and fewer than 10 individual students, but also utilizes complementary suppression and "top and bottom coding" in public reports. This document will guide the reader through the logic of these methods.

### *Suppression*

If any data point reflecting a student count is fewer than 10, the value is suppressed. *N* values of 0 are not suppressed. Totals are retained whenever is possible but still subject to suppression if needed. All student subgroups by which data are disaggregated (e.g., race, ethnicity, FRL, EL etc.) are presented in the report tables even if there are no data for categories.

### *Top and Bottom Coding*

The NDE currently reports >95% for academic outcome percentages over 95% (top coding) and <5% for any percentages less than 5% (bottom coding). Academic outcome values less than 5% and greater than 95% are considered as extreme values.

## Secure Methods of Transmitting Data Electronically

The Bighorn Portal (HTTPS)

Secure File Transfer Protocol (SFTP)

File encryption and separate secure transfer of key

Infinite Campus

# Appendix A—Federal and State Statute and Regulations Related to Education Privacy

## Federal Statute and Regulations

The Family Educational Rights and Privacy Act (FERPA) is the main federal statute and regulations that protect student privacy. The statute is found in the U.S. Code (USC) at 20 USC §1232g. Regulations are found in the Code of Federal Regulations (CFR) at 34 CFR §99.

## State Statute and Regulations

NRS 288.267 requires NDE to adopt policies and procedures consistent with state and federal laws related to the privacy of student data, including, without FERPA and its associated regulations.

NRS 388.268 requires NDE to establish, publish and make publicly available on its Internet website an index of the data elements in Nevada's automated system of accountability information pursuant to NRS 385A.800.

NRS 388.272 requires contracts entered into by NDE that provide for the disclosure of student PII to include (1) provisions specifically to protect the privacy and security of the PII and (2) a penalty for intentional or grossly negligent noncompliance with the terms of the contract, including, without limitation, provisions for termination of the contract and for the payment of monetary damages for any breach of the terms of the contract.

NRS 388.273 requires NDE, in consultation with various stakeholders like school districts and charter schools, to adopt a plan that provides for the security of any data concerning pupils that is collected, maintained, and transferred by the NDE.

NAC 392.306, 392.311, 392.320, 392.325, and 392.330 state that the terms "directory information, "disclose/disclosure," "parent," "personally identifiable information," and "record," respectively, as used this section of regulations, have the meanings ascribed to them in FERPA.

NAC 392.315 states that "education record" has the meaning ascribed to it in FERPA, but further elaborates that the term includes, without limitation:

1. Academic work completed by a pupil.
2. Records indicating a pupil's level of achievement, including, without limitation, his or her grades.
3. Records of a pupil's attendance at school.
4. A pupil's results on standardized intelligence, aptitude and psychological tests.
5. Results from interest inventories completed by a pupil.
6. A pupil's health records.
7. Information concerning a pupil's family and residence.
8. Records concerning a pupil's participation in activities sponsored by the school, special programs and support services.
9. Ratings and observations of a pupil by teachers, counselors and employees of a school district who transport pupils.
10. Reports of serious or recurrent behavior patterns of a pupil which have been verified.

11. Records, ratings and observations recorded by a counselor that are accessible by or revealed to any other person except for a substitute for the counselor.
12. The records of a child who is homeschooled that are maintained by a school district or a person acting for the school district.

NAC 392.340 states that specified provisions of Nevada Administrative Code (NAC) related to education records apply to all schools, including schools that have closed and deposited their records with the superintendent of the school district for the county in which the school was located.

NAC 392.345 outlines how a parent can inspect and review their child's records, and also requires school districts to maintain a list of the types and locations of the education records it collects, maintains or uses.

NAC 392.350 Confidentiality of personally identifiable information; maintenance of permanent record; disclosure under certain circumstances. (NRS 385.080, NRS 392.029)

1. Each school district shall:

(a) Protect the confidentiality of personally identifiable information at its collection, storage, disclosure and destruction;

(b) Appoint one person to assume responsibility for ensuring the confidentiality of all personally identifiable information;

(c) Train or instruct all persons collecting or using personally identifiable information regarding the policies and procedures to be followed concerning such information; and

(d) Maintain a current listing for public inspection of the names and positions of those employees of the district who have access to personally identifiable information.

2. Each school district shall:

(a) Inform the parents when the personally identifiable information is no longer needed to provide educational services to the pupil; and

(b) Maintain a permanent record of the pupil's name, address, telephone number, grades, attendance, classes the pupil attended, grades he or she completed and the year he or she completed them.

3. Subject to the limitations provided by 34 C.F.R. §§ 99.33 to 99.36, inclusive, personally identifiable information may be disclosed to a court of competent jurisdiction or a person or entity pursuant to an order entered by a court of competent jurisdiction or pursuant to a lawfully issued subpoena, if the school district makes a reasonable effort to notify the parents before complying with such an order or subpoena.

(Added to NAC by Bd. of Education by R064-97, eff. 12-10-97)

NAC 392.355 Disclosure of directory information. (NRS 385.080, NRS 392.029)

1. A school district wishing to disclose directory information shall allow a reasonable time after giving notice of the school district's intent to disclose that information for parents to inform the school district in writing that any or all of the information designated should not be released.

2. If a parent informs the school district in writing that any or all of the information should not be released with respect to his or her child, the school district shall not disclose such information concerning that pupil.

3. If a parent does not object, the school district may disclose such information.

(Added to NAC by Bd. of Education by R064-97, eff. 12-10-97)

NAC 392.360 School districts to adopt appropriate policies and procedures. (NRS 385.080, NRS 392.029) Each school district shall adopt policies and procedures so that parents may exercise the rights set forth in 20 U.S.C. § 1232g(a), 34 C.F.R. Part 99 and NAC 392.301 to 392.355, inclusive.

**NAC 392.350 Confidentiality of personally identifiable information; maintenance of permanent record; disclosure under certain circumstances. (**NRS 385.080**,** 392.029**)**

1. Each school district shall:

(a) Protect the confidentiality of personally identifiable information at its collection, storage, disclosure and destruction;

(b) Appoint one person to assume responsibility for ensuring the confidentiality of all personally identifiable information;

(c) Train or instruct all persons collecting or using personally identifiable information regarding the policies and procedures to be followed concerning such information; and

(d) Maintain a current listing for public inspection of the names and positions of those employees of the district who have access to personally identifiable information.

2. Each school district shall:

(a) Inform the parents when the personally identifiable information is no longer needed to provide educational services to the pupil; and

(b) Maintain a permanent record of the pupil's name, address, telephone number, grades, attendance, classes the pupil attended, grades he or she completed and the year he or she completed them.

3. Subject to the limitations provided by 34 C.F.R. §§ 99.33 to 99.36, inclusive, personally identifiable information may be disclosed to a court of competent jurisdiction or a person or entity pursuant to an order entered by a court of competent jurisdiction or pursuant to a lawfully issued subpoena, if the school district makes a reasonable effort to notify the parents before complying with such an order or subpoena.

(Added to NAC by Bd. of Education by R064-97, eff. 12-10-97)