



# STUDENT DATA PRIVACY

BROUGHT TO YOU BY EDUTECH AND NDETC

# OBJECTIVES OF THIS PRESENTATION

1. Raise awareness of the importance of protecting student data and privacy
2. Provide an overview of the flow of student data in schools and the state
3. Provide a sample model school policy for protecting student data
4. Provide resources for schools to use for staff training and to inform parents about how student data is collected, used and protected.



# WELCOME

- Who is talking about student data privacy?
  - ✓ Legislators
  - ✓ Parents
  - ✓ Media
  - ✓ State Educational Leaders
  - ✓ Gates Foundation
  - ✓ Department of Education
  - ✓ School Leaders
  - ✓ Teachers

© MARK ANDERSON, WWW.ANDERSTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."

# SCENARIOS

The image features a blue gradient background with white circuit-like lines in the corners. These lines consist of straight paths that branch out and terminate in small circles, resembling a network or data flow diagram.



# SCENARIO 1

- ✓ Your school board approved directory information for your school that includes student name, grade level, birth date, parent name, address, photo and phone number. Directory information is allowed to be publically shared. Do you need to provide notice about this directory information and are you required to provide an opt out option for students/parents?
- ✓ Schools must provide notice and can decide how to provide the notice. It could be in a special letter or in the student handbook for example. An opt out option is required to be available for parents and should be done in writing.

## SCENARIO 2

- ✓ During finals, the chemistry teacher posts students grade on the hallway bulletin board in the following format:

Student ID

Grade

Does this practice violate FERPA?

- ✓ Yes, FERPA applies to information directly related to a student. This includes grades. You may not do this with student id or any other code for the student name.

## SCENARIO 3

- ✓ A teacher keeps a personal file, it could paper or electronic, of notes they have taken on a student during the school year. The notes include dates and behaviors of the student. The student notices the practice and tells their parents. The parents request a copy of the file. Does the information need to be turned over to the parents?
- ✓ No. The notes are known as “sole possession notes” and are not covered by FERPA if they are not part of the student record, are used only by the teacher or school official and are not shared with others.



## SCENARIO 4

- ✓ Under new North Dakota law, what local process is required when sharing data with third party vendors such as an alert system provider or online assessment company?
- ✓ Schools need to adopt or update a policy regarding the protection of student data. The policy must require that permission be obtained from the board before student data is shared with an outside entity. Upon approval from the board, the student data may be shared with the third party vendor.



# ACRONYM ROUND UP

# CIPA

- **Children's Internet Protection Act**

- ✓ **Addresses concerns about children's access to obscene or harmful content over the Internet.**

- ✓ Protection measures include:

- ✓ Obscene, child porn & harmful to minors

- ✓ Schools must certify:

- ✓ Their online policy includes monitoring and they educate minors on appropriate online behavior



# COPPA

- **Children's Online Privacy Protection Act**

- ✓ **Controls data collected from children 13 & under**

- ✓ Requires companies to post a clear privacy policy on their site, provide direct notice to parents and obtain permission before collecting information from children under 13.
    - ✓ O365 accounts are schools owned and approved for students.
    - ✓ Teachers and school officials need to authorize for all educational programs.
    - ✓ NO commercial purposes are allowed with student data.

# PPRA

- **Protection of Pupil Rights Amendment**
  - ✓ **Outlines what information students can be asked on federally funded surveys or evaluations.**
    - ✓ In order to administer surveys, schools must be able to show the survey materials used and get consent.
    - ✓ Consent can be done in one action with back to school forms if known in advance.
    - ✓ Opt out rights exist.
    - ✓ Schools are restricted on what they can share. NDCC allows sharing with NDUS and military recruiters.

# FERPA

- **Family Educational Rights and Privacy Act**

- ✓ **Outlines parent's rights to their child's education record and restricts access and use of that information.**

- ✓ Inspect and review child's record

- ✓ Request corrections or deletions for anything that is inaccurate

- ✓ Consent, or deny, disclosure of some of child's information in certain situations

- ✓ When child turns 18, the rights belong directly to him or her.

- ✓ School directory information is not protected.

- ✓ Exceptions for school transfers, judicial orders, health/safety reasons and others.



# PII

- **Personally Identifiable Information**
  - ✓ Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
    - ✓ Includes student name, names of family members, household address, date/place of birth, SSN, digital files. etc.

# NSLA

- **National School Lunch Act**

- ✓ **Protects free and reduced lunch data.**

- ✓ Stricter than FERPA

- ✓ Strict confidentially on free and reduced lunch as well as drug and alcohol prevention and treatment services.



FPCO


- **Family Policy Compliance Office**

- ✓ **Administers two federal laws that provide parents and students with certain privacy rights**

- ✓ FERPA

- ✓ PPRA





# STUDENT DATA PRIVACY AND SECURITY

NDSBA – MODEL/SAMPLE POLICY – TO BE  
CUSTOMIZED BY EACH SCHOOL DISTRICT

# DEFINITIONS

- Directory Information
- Education Record
- Eligible student
- Parent
- Permanent record
- Legitimate educational interest
- Personally Identifiable Information (PII)
- Record
- School official
- FERPA

# DESIGNATION AND RESPONSIBILITIES OF PRIVACY OFFICERS

- Superintendent (or designee) is Chief Privacy Officer
  - Responsibilities
    - Submitting to Board requests for release of student information
    - Maintain master list of individuals and entities (by title) with access to information
    - Ensure that the master list remains current and is manageable to maintain
    - Designate privacy officers at district and school level
- Designated Privacy Officers
  - Responsibilities
    - Maintain list of school personnel (by title) who have access to student PII
    - Submitting to superintendent, for board approval, new requests to share information not required by law.
    - Ensure access is granted only for legitimate educational purposes and according to policy and law
    - Enforcing data protection policies
    - Providing a list of students who have opted-out of directory information to teachers and other district staff that need to know.



# INFORMATION RELEASE SAFEGUARDS

- **Access by Parents and Eligible Students:** To ensure compliance with parental and eligible student access under FERPA, the District shall:
  - Comply with requests in reasonable time (no more than 45 days)
  - Board develops procedures for parent/eligible student review and to amend record
    - Need to include procedures to verify identity of parent/eligible student requesting review
  - Spelled out in board approved regulations and disseminated annually.

# CLASSROOM USE OF INSTRUCTIONAL TOOLS REQUIRING RELEASE OF STUDENT INFORMATION

- Teachers are encouraged to use tools that allow an alias or that do not require sending directory information (DI) or PII
- Teacher submits request to building-level privacy officer if the instructional tool requires release of DI, other than or in addition to name, or PII.
- Building level privacy officer checks master list of approved entities
- If entity is not on the list
- options:
  - Deny the request
  - Submit request to superintendent for board approval
- If teacher is authorized to use the instructional tool, the building level privacy officer shall ensure that the teacher complies with parental consent if requirements and DI opt-out requests.

# DATA BREACHES

- District employees are responsible for informing the privacy officer of known or suspected breach of PII
- Privacy officer contacts the Chief Privacy Officer (Superintendent) when aware of breach
- Chief Privacy officer determines if enactment of the district's data breach response procedures according to policy or procedures, is appropriate .



# INFORMATION STORAGE AND DESTRUCTION

- Student records reviewed annually
  - Records not necessary for:
    - Progression to next level
    - College entrance purposes
    - Extracurricular participation
    - Disciplinary purpose

Records not part of the Permanent Record shall be shredded and/  
or destroyed

# EXCEPTIONS

- Records reasonably related to litigation or potential litigation. Kept for 6 years after student turns 18.
- Bullying reports
- Concussion documentation
- Executive session tapes (retain 6 months)
- PowerSchool Records
- Special Education records (retain as per IDEA 5-7 years)

# DIRECTORY INFORMATION

- District may disclose directory information without parent consent providing the district has:
  - Defined directory information
  - Given notice to parents
  - Provided a reasonable amount of time for parents to opt-out
    - Usually done at beginning of school year and/or when a student enrolls. At least 10 days is considered reasonable
  - Directory information should only be released and used for purposes specified in the release request. The new approved entity is added to the master list of entities having access to student directory information.
  - Board develops criteria in regulations for approving and denying requests for DI and PII \*



# BOARD APPROVES RELEASE OF DIRECTORY INFORMATION AS FOLLOWS:

- publication on website
- to board approved vendors
- to military and college recruiters
- to official district newspaper
- to school-affiliated groups for communication and fundraising
- school-sponsored student publications
- when receives and approves a DI release request

# PERSONALLY IDENTIFIABLE INFORMATION (PII)

- Any 3<sup>rd</sup> party request for PII must have board approval unless the 3<sup>rd</sup> party is required by state or federal law to receive it.
- Includes school employee who wishes to share PII. Must contact school privacy officer for consideration.

# PARENTAL/ELIGIBLE STUDENT CONSENT NOT REQUIRED

- Disclosure concerns sex offenders required to register and district has a need to disclose the student's status for safety.
- Records de-identified by the district-if provided to third party
  - included on the master list of individuals and entities having access to information.
- Another school the student seeks to attend or is already enrolled in.
- School official with legitimate interest (need to know)
  - name/title should be on the master list of people with access



# PARENTAL CONSENT NOT REQUIRED

- To organizations conducting a study as long as there is a written agreement in accordance with the law. If it includes a survey of students, parents notified and consent may be required
- Health or safety emergency
- Accrediting bodies for accreditation

# CONSENT NOT REQUIRED

- Comply with judicial order or subpoena
  - District should make reasonable attempt to contact parent/eligible student unless the court order instructs otherwise
- To a court without court order if district initiated legal action against parent or student or parent/student has initiated legal action against the school
- To a parent of an eligible student who is also a “dependent student”
  - Claimed on parent’s tax return.
- State, federal and local education authorities for audit and/or evaluation purposes to determine compliance.

# WHEN PARENTAL/ELIGIBLE STUDENT CONSENT IS REQUIRED

- When board has approved the release of PII to an entity not meeting the definition of a school official and not meeting the exception to consent requirements of FERPA
- When the board has approved DI, other than or in addition to name, or PII release to an online provider for commercial purposes and students are under age 13.



# CONSENT REQUIRED:

WHEN ADMINISTERING A SURVEY FUNDED IN ANY WAY BY THE US DEPT. OF EDUCATION AND CONCERNING THESE AREAS

- Political affiliations or beliefs of the student or parent
- Mental or psychological problems of the student or parent
- Sex behaviors and attitudes
- Illegal, anti-social, self incriminating, or demeaning behavior
- Critical appraisals of other individuals with whom the student has close family relationships
- Legally recognized privileged or analogous relationships - lawyer, physician, minister.
- Religious practices, affiliations or beliefs of student or parent
- Income (other than that required by law to determine eligibility for programs or services)

# INDIVIDUAL EDUCATIONAL PLANS (IEP'S) AND 504'S

- Sharing student information necessary for:
  - developing
  - amending
  - implementing
- not subject to board approval
- Services are provided pursuant to state and federal law

# POLICY VIOLATIONS

- By school personnel
  - Explain consequences
- By a third party
  - Consequences



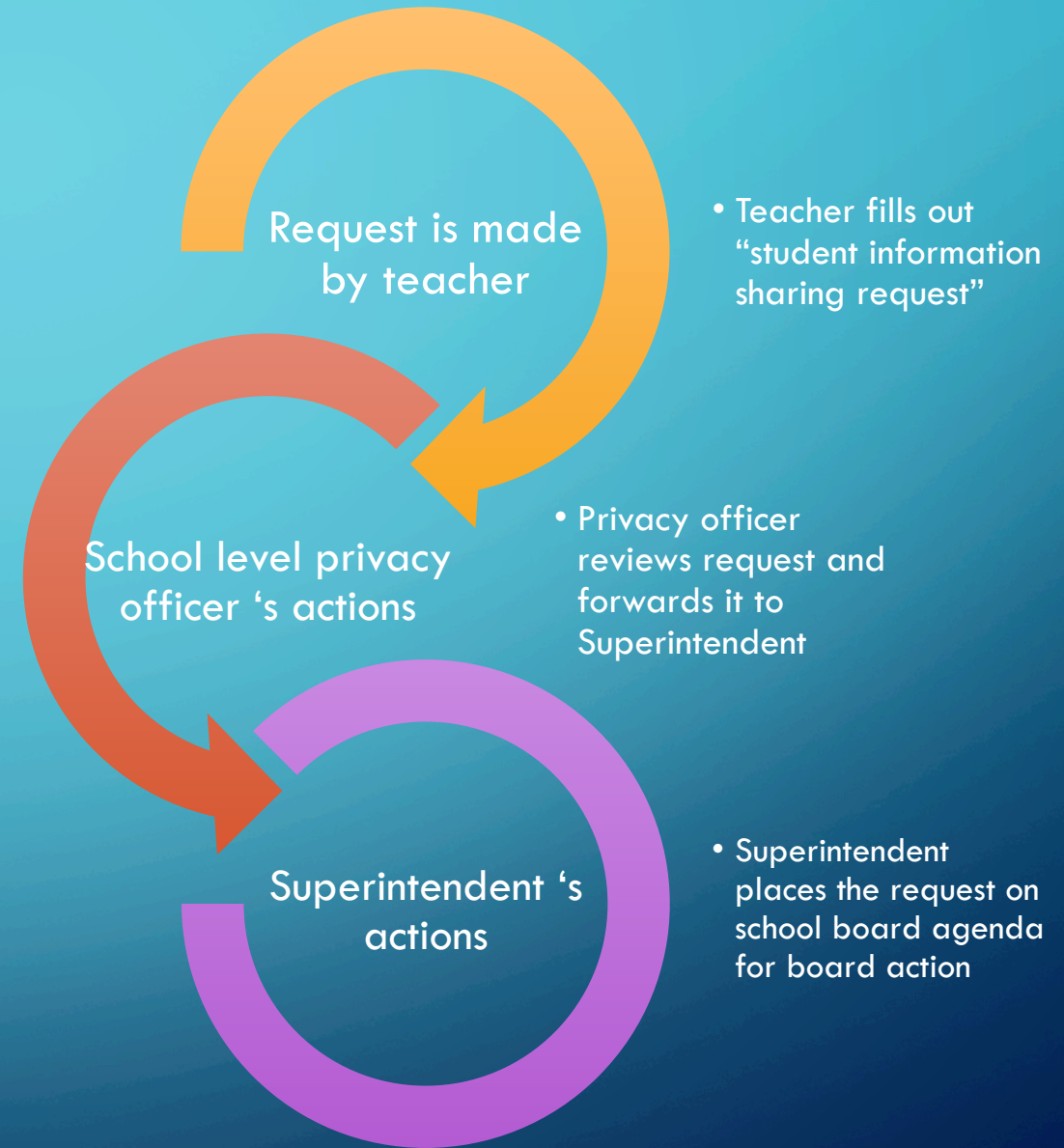
# TRAINING

- Provide training on confidentiality requirements and consequences for breaching confidentiality.
- School staff employed and volunteering
- Procedures for staff to follow when requesting to release student information as outlined in the policy.

# NDSBA TEMPLATE – STUDENT INFORMATION SHARING REQUEST FORM

- Worksheet for district use for requesting data sharing with a third party.
- Provides a workflow and outlines responsibilities.
- Helps determine and ensure the legitimate educational interest of the request.
- May be customized to fit the individual district's use.

# TEACHER REQUESTS TO SHARE DATA WITH 3<sup>RD</sup> PARTY





The background is a gradient of blue shades, from a lighter teal at the top to a darker blue at the bottom. In the four corners, there are decorative white line-art patterns resembling circuit traces or data paths, with small circles at the end of the lines.

# CRITERIA FOR APPROVING AND DENYING DI AND PII RELEASE REQUESTS

# FINDING ALTERNATIVES TO RELEASE

- Board should identify alternatives to release of PII or DI -if possible
- Asking requestor to disseminate material directly through the school's systems
- De-identify data before release

# REASONS FOR RELEASE OF DI OR PII

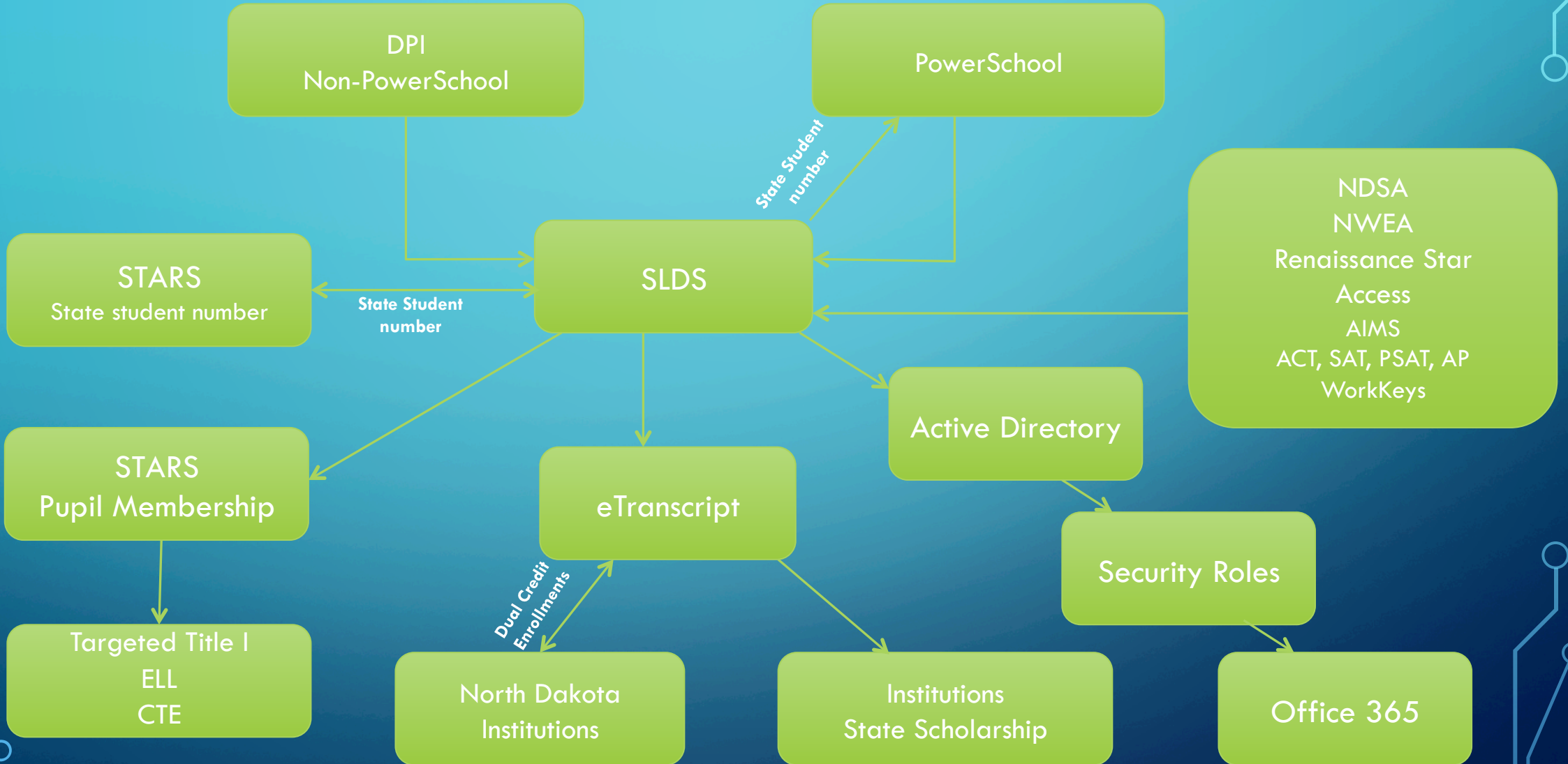
- should further the mission of the school
- support development of:
  - students
  - specific district school
  - the District
  - school sponsored program



# CRITERIA FOR DENYING RELEASE

- Attacks ethnicity, race, religion, or class protected by the law.
- Promotes violence, terrorism or other illegal activity
- may substantially disrupt the educational environment
- Poses direct threat to safety of students
- Infringes on the rights of students; potentially libelous or invades privacy
- Has political purpose defined as:
  - support or opposition to statewide initiated or referred measure, constitutional amendment, a political subdivision ballot measure, or election or nomination of a candidate for public office.

# STUDENT DATA FLOW



# DATA AGREEMENTS

- DPI

- <http://www.dpi.state.nd.us/resource/NDSLEDS.shtm>
  - NWEA
  - DIBELS
  - AIMSweb

- Data Steward Blog

- <http://www.ndetc.k12.nd.us/dsteward/files/2015/01/ND-SLDS-Integration.pdf>
  - Renaissance Star - support@renaissance.com

- LEA Authorization for Student Level Data

- Template available on EduTech website



# MANAGEMENT OF DATA AGREEMENT

- District and Involved Party
  - Original for district
    - How and where to store
  - Involved Party – copy
- Update or Review yearly

# SECURITY ADMIN

- Superintendent or designated individual[s]
- SLDS and eTranscript
  - Yearly process July 15
    - Review individuals and permissions granted
    - Reauthorize individuals
- Will not allow districts to authorize new individuals at this time.
  - An EduTech help desk ticket will need to be submitted

# STAFF DEPARTURE CHECKLIST

- In Application
  - PowerSchool - No longer Active (staff)
    - Office 365
      - Auto Users - Staff with teacher license number
    - STARS
  - In Security App. by District Security Admin
    - SLDS
    - eTranscript
  - In My Admin Security App. by Building facilitator or Tech Director
    - Office 365
      - Non Auto Users - Admin Assistants
  - Third party applications
    - ViewPoint
    - Alert Solutions
    - Blackboard Connect/Alert Now
    - Honeywell/Edline/Instant Alert
    - Others
- Third party applications
  - ViewPoint
  - Alert Solutions
  - Blackboard Connect/Alert Now
  - ParentLink
  - Honeywell/Edline/Instant Alert
  - Others
- Change shared passwords
  - NWEA
  - STARS



**EDUTECH**  
education technology services



## Student Data Privacy Resources

[www.edutech.nodak.edu/sdp](http://www.edutech.nodak.edu/sdp) • #sdp

[www.dpi.state.nd.us/resource/NDSLEDS.shtm](http://www.dpi.state.nd.us/resource/NDSLEDS.shtm)  
[bitly.com/stardataslds](https://bitly.com/stardataslds)

**EDUTECH**  
education technology services



## Contact EduTech Help Desk

[www.edutech.nodak.edu/help](http://www.edutech.nodak.edu/help)

800.774.1091 • 701.451.7400

[help@k12.nd.us](mailto:help@k12.nd.us)



QUESTIONS?





THANK YOU!