Student Restraint and Seclusion (SRS) Training Manual

Table of Contents

Section 1: Overview **3**
File Layout 3
Business Rules: Error and Warnings 3
Warnings 3
Errors 3
Exception Requests 3
Reporting Exceptions 3
Identity Management Roles 3
Section 2: Data Pipeline **4**
No Restraint Events to Report 4
File Upload 5
Format Checker 5
Data File Upload 6
Validation Report 7
Batch Maintenance 8
SRS: Additional Tools 8
Status Dashboard 8
Submit to CDE 9
Download Sign Off Form 9
Edit Record 9
File Extract Download 11
Pipeline Reports 11
Steps 11
Section 3: CEDAR/COGNOS **12**
General 12
Accessing & Navigating CEDAR 13

Access via Identity Management (IdM) webpage 13
Access via link in Data Pipeline 13
Navigating CEDAR 13
Section 4: Syncplicity & PII 13
PII 13
Syncplicity 14
Steps 14
Section 5: SRS Data Use and Privacy Guidelines 14
Data Privacy Guidelines 14

Section 1: Overview

The Student Restraint and Seclusion collection collects the number of students restrained along with the type and duration of the restraint.

Visit the Student Restraint and Seclusion website to review the collection timeline, file layouts, resources, and more information.

File Layout

For a complete list of data field and definitions, review the Student Restraint and Seclusion file layout on the SRS website.

Business Rules: Error and Warnings

Business rules are the list of errors and warnings that are checked when a file is uploaded for a specific data collection. They help ensure data accuracy by alerting you to common coding irregularities. SRS business rules focus on ensuring accurate data, address common data irregularities and check for file layout specific requirements.

Warnings

Warnings indicate possible data inconsistencies/coding issues. It is beneficial to review warnings to ensure data is accurately reflected. A collection can be submitted even if warnings are present.

Errors

Errors *must* be addressed to submit data for a given data collection such as SRS. Errors can be addressed by updating the related data field in the SIS and reuploading the file or by requesting a reporting exception.

Exception Requests

Reporting Exceptions

Reporting Exceptions, or 'exceptions' refer to overriding Data Pipeline errors. CDE occasionally overrides these business rule errors because, although errors are legitimate, the case needs to be corrected to accurately reflect the SRS record. This occurs under unique circumstances when a record does not follow the anticipated coding patterns outlined in the business rules for a periodic file. The record must fall within the parameters of the data collection for an exception to be granted.

When an exception is requested and approved, *the record causing the error does not change*, but instead it is ignored to allow the error to clear.

Identity Management Roles

Each district must have at least one user assigned the SRS LEA Approver role in order to complete the collection. Your district's Local Access Manager (LAM) assigns accounts/privileges in IdM for your district. LAMs, see the IdM website for access management instructions.

Application	Collection	User Role	Access Level	Notes
Pipeline	SRS	LEA User	Upload SRS file	Users with this role can complete most of the SRS collection but will need support from a LEA Approver for a few steps.
Pipeline	SRS	LEA Approver	Submit data, download sign-off form	At least one person in the district must have this role.
Pipeline	Any	LEA Viewer	View CEDAR/COGNOS reports related to the assigned collection – cannot edit data.	Useful role for district staff who need access to collection related CEDAR/COGNOS reports for data validation but are not actively completing the data collection.

***Note**: A user may only have one role per collection in IdM. Users assigned to more than one collection role will not be able to login to Data Pipeline correctly because the user roles are competing and will lock the account.*

Section 2: Data Pipeline

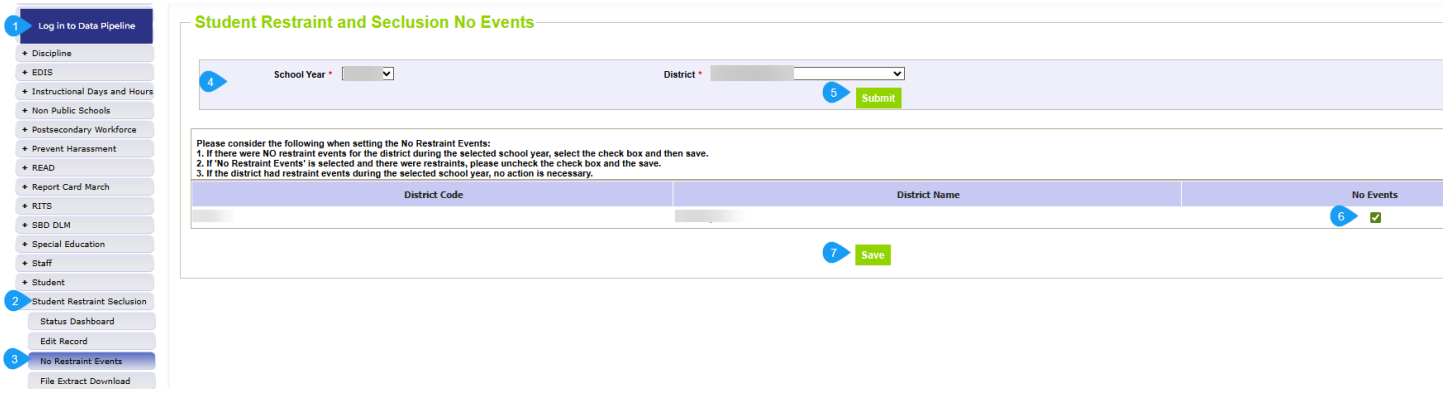
This section covers in detail the various data pipeline screens and functions used by data respondents when completing a collection. Check out the Respondent Training Page for additional information applicable to all data pipeline collections.

No Restraint Events to Report

These steps are **ONLY** used if the LEA has no SRS events to report for the collection year.

Steps

1. Login to Data Pipeline
2. *Select Student Restraint Seclusion*
3. Select *No Restraint Events*
4. Complete the drop-down menus
    a. School Year: collection year
    b. Organization/LEA: Your district
5. Select *Submit*
6. Check *No Events*
7. Select *Save*



Note: *LEAs that have no SRS events **MUST** still Submit to CDE and complete the Sign off Form.*

File Upload

These steps can be used to upload any file into data pipeline.

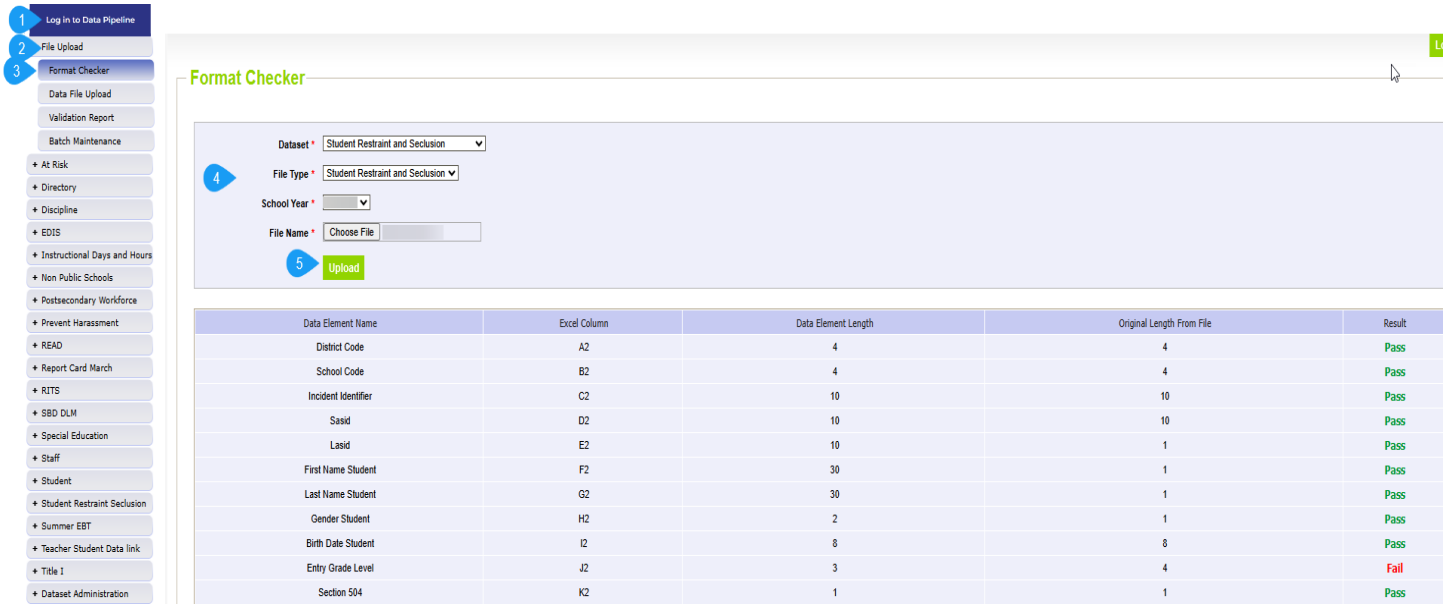
Format Checker

The format checker can be used to ensure a file is in the proper format for the given file type and school year. The format checker screen shows data fields that are the *incorrect length based on the first row of data*. This may indicate the file layout does not have the data elements listed in the correct order or that leading zeros are missing for some data fields.

Note: *It is possible for a file to pass the format checker and still have underlying errors.*

Steps

1. Login to Data Pipeline
2. Select *File Upload*
3. Select *Format Checker*
4. Complete the Dropdown menus, indicating the specific file you are uploading.
    a. Dataset: (e.g., Student Restraint and Seclusion)
    b. File Type: (e.g., Student Restraint and Seclusion)
    c. School Year: collection year (Note: Other years may be available, so please ensure you select the correct year)
    d. File Name: Choose File → Select file from your computer
        i. .csv, .xls, .xlsx (.xlsx is preferred)
        ii. Spaces are not allowed in the file name
5. Select *Upload*
6. Review the on-screen results to look for data elements that failed the format check.



Data File Upload

The data file upload screen is where a LEA uploads the collection file(s).. LEAs may upload files multiple times throughout the collection to address errors/warnings. Most collection files are extracted from a LEA's student information system reflecting updates to data in the student information system on a new file extract. LEAs are encouraged to use a naming convention for files saved on their local system that includes the upload date so they can track changes made to these files throughout the collection.

Upon completing the file upload steps listed below, a message will be displayed across the top of the screen indicating a batch number or that there was an error uploading the file. Data pipeline sends an email to data respondents once the file has been processed. This email will indicate the number of records uploaded into data pipeline and the number of errors related to this file upload. If you receive an email indicating a file upload error, double check the formatting of your file and try again. Alpha characters or symbols included in data fields that are numeric only is a common cause for file uploads to fail. This includes if an alpha character/symbol in a single data field for a single row of data.

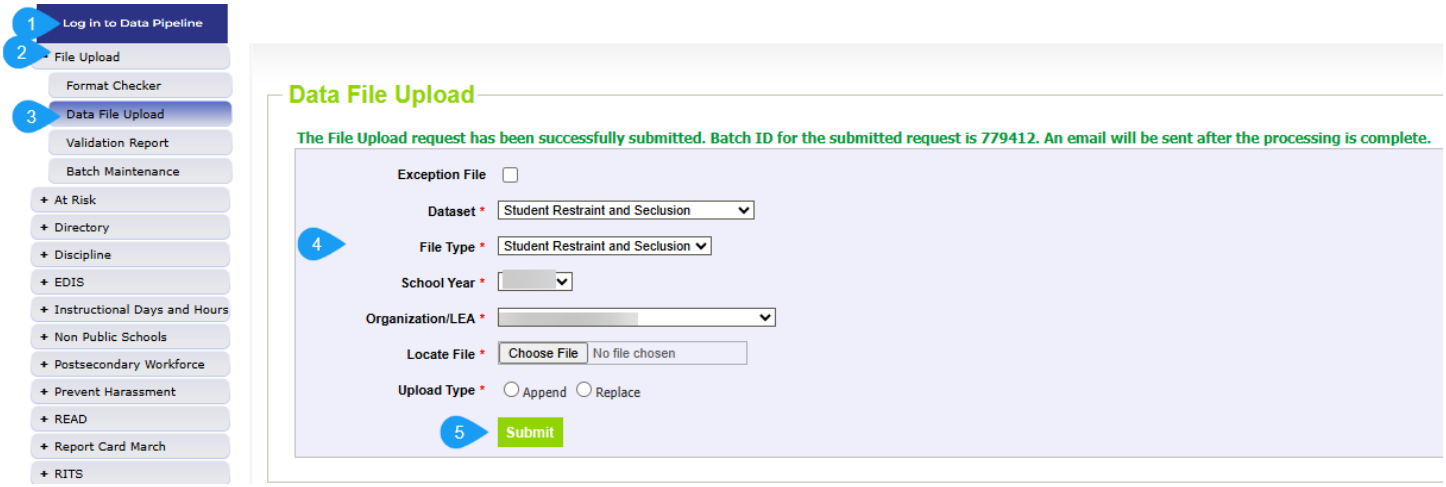
Note: *File uploads are the preferred method for updating data.*

Steps

1. Login to Data Pipeline
2. Select *File Upload*
3. Select *Data File Upload*
4. Complete the Dropdown menus, indicating the specific file you are uploading.
    a. Dataset: (e.g., Student Restraint and Seclusion)
    b. File Type: (e.g., Student Restraint and Seclusion)

c. Tag: None
d. School Year: collection year
e. Organization/LEA: Your district
f. File Name: Choose File → Select file from your computer
    i. .csv, .xls, .xlsx (.xlsx is preferred)
    ii. Spaces are not allowed in the file name
g. Upload Type = Append or Replace
    i. Relace is recommended

5. Select *Submit*

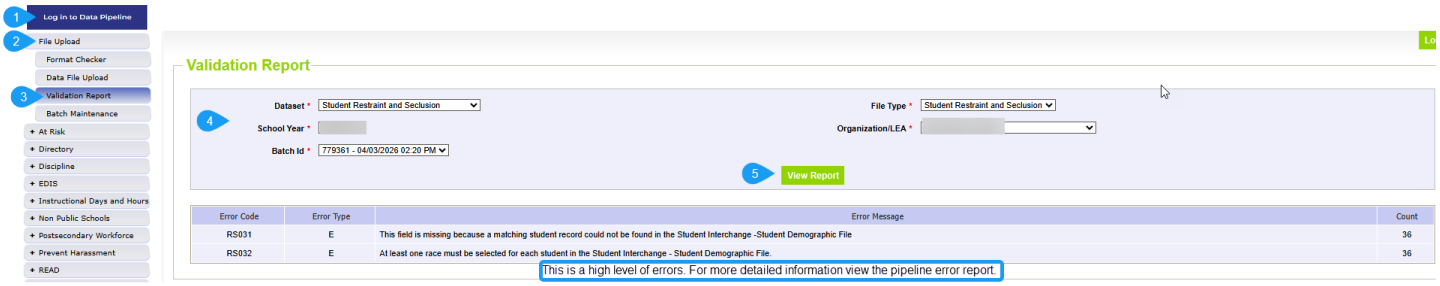


Validation Report

The Validation Report shows a high-level view of the errors for a specific file upload. Data respondents may find this report to be less beneficial than the more detailed data pipeline error report.

Steps

1. Login to Data Pipeline
2. Select *File Upload*
3. Select *Validation Report*
4. Complete the Dropdown menus, indicating the specific file you are reviewing.
    a. Dataset: (e.g., Student Restraint and Seclusion)
    b. File Type: (e.g., Student Restraint and Seclusion)
    a. School Year: collection year
    c. Organization/LEA: Your district
    d. Batch ID: number and date of the specific file upload as indicated on the data file upload screen and/or the subsequent email.
5. Select *View Report*

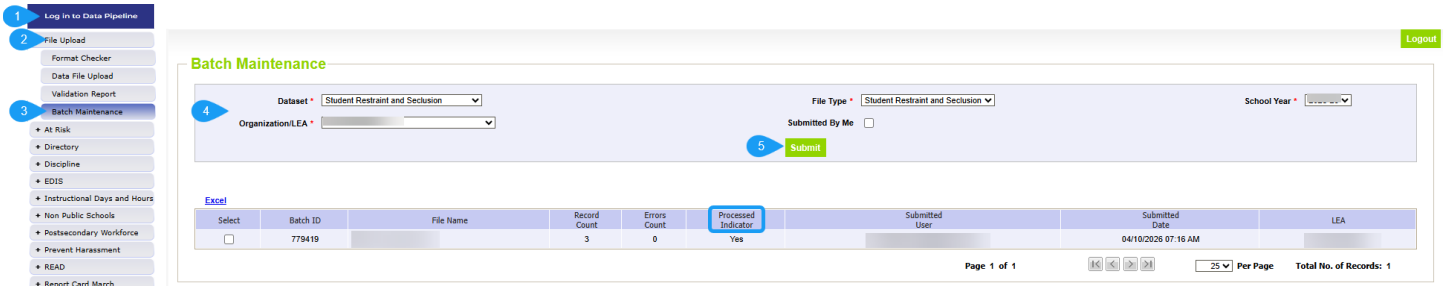


Batch Maintenance

This screen provides information regarding the status of a file upload and can be used to determine if a file has completed processing. If a file is taking a significant amount of time to process (an hour or more) and you have not received an automated email from Data Pipeline regarding the file, please contact the collection lead for support.

Steps

1. Login to Data Pipeline
2. Select *File Upload*
3. Select *Batch Maintenance*
4. Complete the Dropdown menus, indicating the specific file you are reviewing.
    a. Dataset: (e.g., Student Restraint and Seclusion)
    b. File Type: (e.g., Student Restraint and Seclusion)
    b. School Year: collection year (Note: Other years may be available – select the desired year)
    c. Organization/LEA: Your district
5. Select *Submit*



SRS: Additional Tools

Status Dashboard

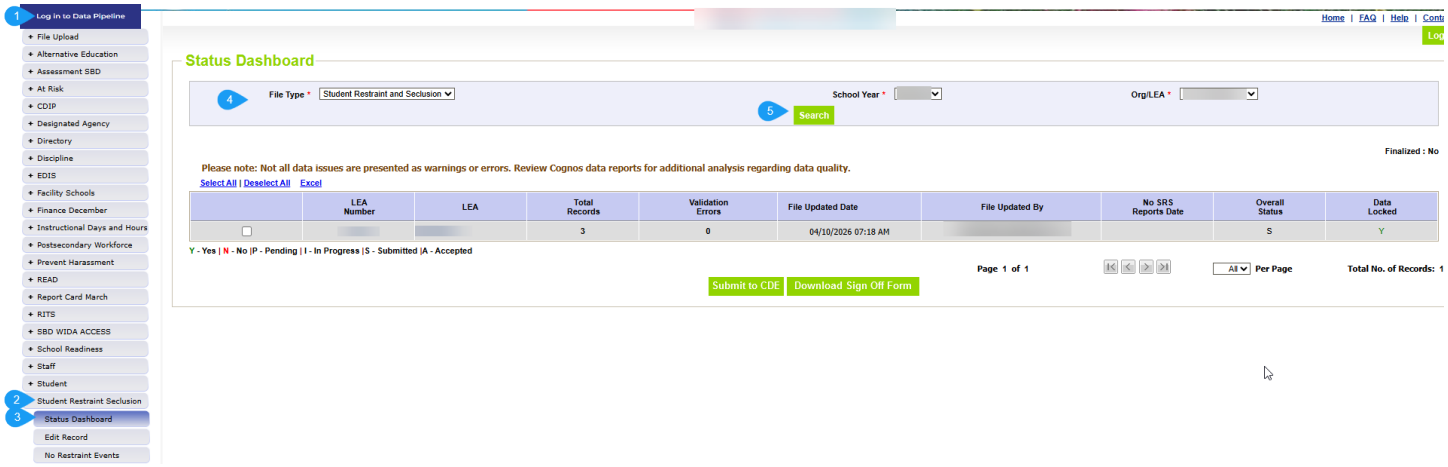
The status dashboard shows the last date a file was updated, the quantity of validation errors, and if data has been submitted (locked) for a collection. The Student Restraint and Seclusion status dashboard is also used by data respondents with the LEA Approver role for SRS to submit data to CDE and download the Superintendent Verification (Sign-Off) form at the end of the collection.

Steps

1. Login to Data Pipeline
2. *Select Student Restraint Seclusion*
3. Select *Status Dashboard*
4. Complete the drop-down menus

a. File Type: desired file (Student Restraint and Seclusion)
b. School Year: current year
c. Organization/LEA: your district

5. Select *Search*



Submit to CDE

Respondents with the LEA Approver must press the 'Submit to CDE' button to signify their district has error free data and has validated their data, completing the SRS collection. LEA Approvers can check that the data has been submitted by reviewing the status dashboard screen, specifically looking for the 'Overall Status' to change to 'S' for submitted.



Download Sign Off Form

Respondents with the LEA Approver must download the Superintendent Verification form using the Download Sign Off Form button on the status dashboard screen at the end of the SRS collection. This form is signed by the LEA's superintendent and returned to the SRS collection lead via email. This form cannot be downloaded until the LEA's data is error free and submitted.



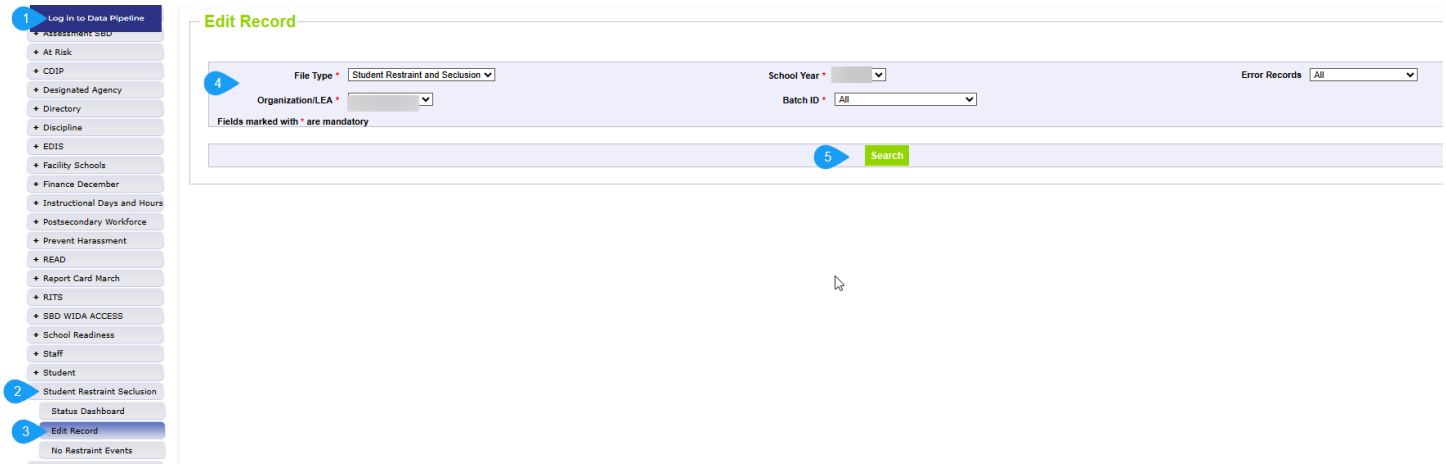
Edit Record

This screen can be used to update a record to a SRS file without uploading a new file. Filters allow you to search for records in error by School Code or by Investigation Identifier. A new file upload will delete any manually edited records, so only use this step if you are no longer planning to upload new data files *or* if you have also updated your file before the new upload.

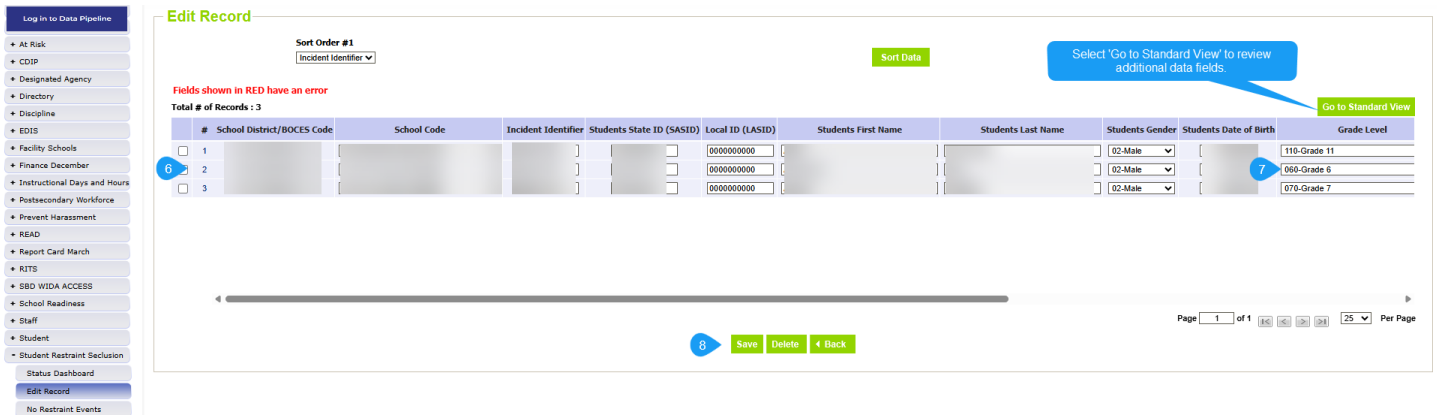
Steps:

1. Login to Data Pipeline
2. *Select Student Restraint Seclusion*
3. Select *Edit Record*

4. Complete the drop-down menus for the desired file.
    a. File Type: Student Restraint and Seclusion
    b. School Year: current year
    c. Organization/LEA: your district
    d. Batch ID
    e. OPTIONAL: Error Records = desired category
5. Select *Search*



6. Check the box indicating the record being updated.
7. Input the updated information into the desired data field. Some fields are drop-down menus and others are text fields.
    a. Use the scroll bar across the bottom of the screen to locate the desired data field.
    b. If the desired data field is not showing, select 'Go to Standard View' to view additional data fields.
8. Select *Save*
    ***Note**: Use the Delete button to delete the entire selected record.*



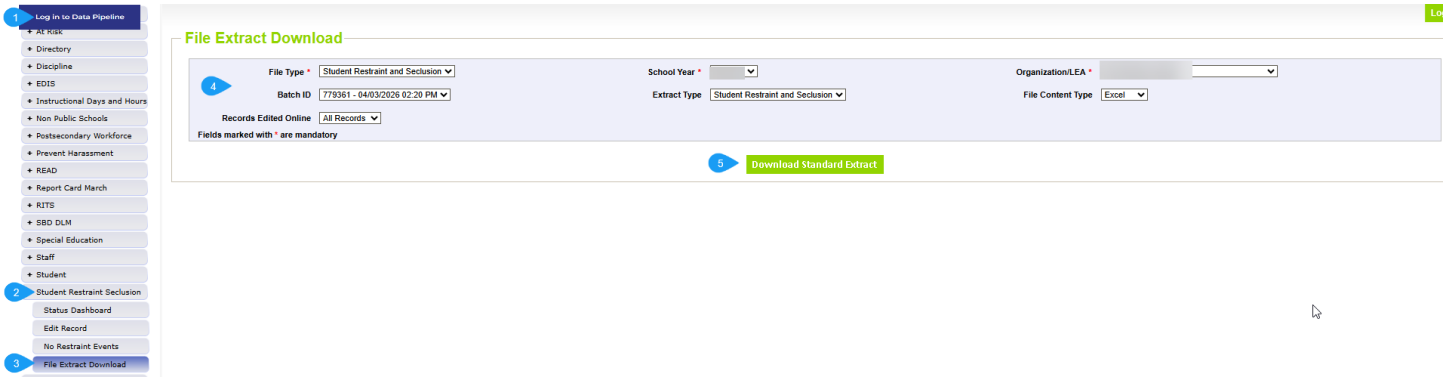
Pro Tip: Use the file extract download feature in data pipeline to download your SRS file after you've finished making any manual updates. This will give you a clean file that includes all updates for your records.

File Extract Download

A copy of a desired Student Restraint and Seclusion file can be extracted from data pipeline for future reference. This is especially beneficial if you want to download a copy of a file after edits have been made to the data, providing a record of those updates.

Steps

1. Login to Data Pipeline
2. *Select Student Restraint Seclusion*
3. Select *File Extract Download*
4. Complete the drop-down menus
    a. File Type: desired file (e.g. Student Restraint and Seclusion)
    b. School Year: current year
    c. Organization/LEA: your district
    d. Batch ID: All (or desired date/time of a file upload)
    e. Extract Type: desired value
    f. File Content Type: CSV, TEXT, or Excel
        i. Excel format recommended
    g. Records Edited Online: All Records or Online Edits
5. Select *Download Standard Extract*
6. Open the downloaded file and/or save it to your computer.



Pipeline Reports

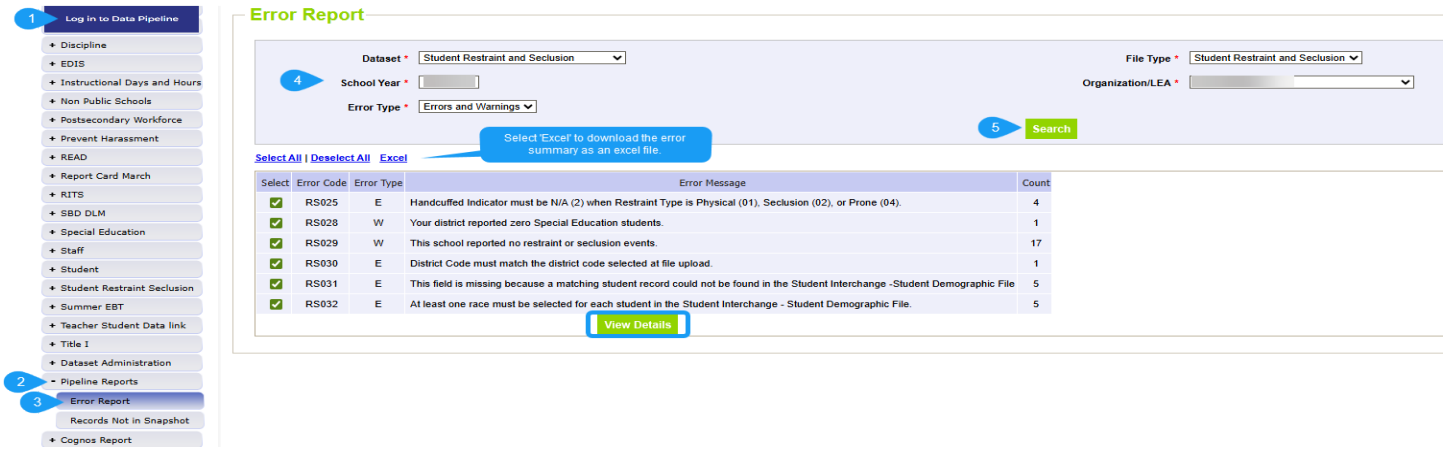
The data pipeline error report is the preferred method for reviewing errors and warnings. Using the pipeline error report LEAs can review a summary of all errors and warnings and a detailed list of records triggering specific business rules. Use the 'View Details' button at the bottom of the pipeline error report summary screen to view the detailed list of records triggering each error or warning. Both the summary screen and the detail error screens can be extracted as an excel document.

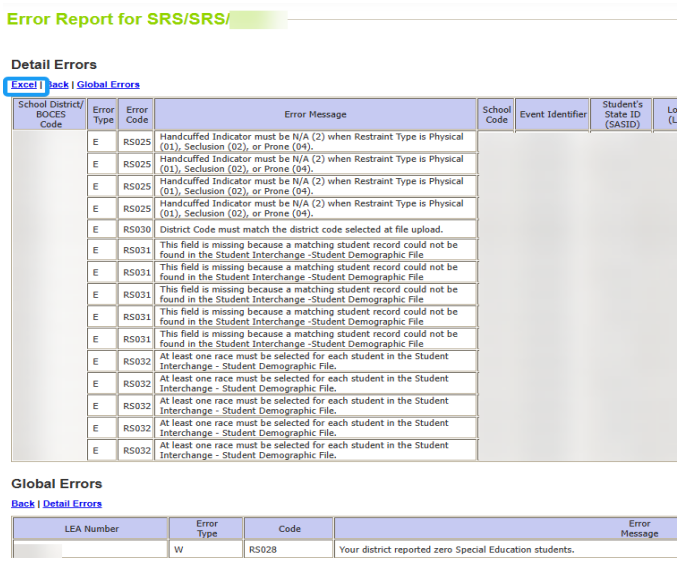
Steps

1. Login to Data Pipeline
2. Select *Pipeline Reports*
3. Select *Error Report*
4. Complete the drop-down menus for the desired file/snapshot
    a. Dataset: Student Restraint and Seclusion
    b. File Type: desired file/snapshot (Student Restraint and Seclusion)

c. School Year: collection year (Note: Other years may be available – select the desired year)
c. Organization/LEA: your district
d. Error Type: Desired type of Business Rules (Errors and Warnings recommended)

5. Select *Search*





Section 3: CEDAR/COGNOS

General

The Colorado Education Data Analysis and Reporting system (CEDAR) is a private, secure system which provides student level data to authorized users. Access to student-level data is limited to educators who have need for such data.

Often CEDAR is referred to as COGNOS since COGNOS is the software currently powering the Colorado Education Data Analysis and Reporting system (CEDAR).

Reports in CEDAR/COGNOS have multiple purposes. Some are used as operational reports to assist data respondents in looking up specific information on records and file errors. Other reports

are used to validate data when finalizing the data collection. Many reports also provide districts with a preview of data that will be published based upon specific data collections.

Student Restraint and Seclusion CEDAR/COGNOS reports are focused on the information needed to accurately report student restraint events. It is important to remember that a file may still have data inaccuracies even if no business rules are triggering for that file. CEDAR reports help districts review their data to look for potential data inconsistencies throughout the SRS collection.

Accessing & Navigating CEDAR

Google Chrome is the preferred browser when working with CEDAR reports. If CEDAR is not loading properly in Chrome, clear the browser history/cookies/cache and try logging in again.

Access via Identity Management (IdM) webpage

1. Go to the IdM webpage
2. Expand the CEDAR accordion.
3. Select the 'Log in to CEDAR' button

Access via link in Data Pipeline

1. Login to Data Pipeline
2. Select the COGNOS Report button on the bottom of the navigation menu on the left.

Navigating CEDAR

Use the navigation bar on the left to open the pipeline reports folder and view specific categories of reports. Reports are organized based upon a user's access permissions in IdM.

Each category file of reports represents reports connected to a specific data collection/IdM user role. SRS Data respondents should have access to the Student Restraint and Seclusion reports. Select the desired report from the list to view the report. Most reports will have an introductory screen with dropdown menus to further refine the data in the report.

Section 4: Syncplicity & PII

PII

Student Personally Identifiable Information (PII) includes, but is not limited to, information that is collected, maintained, generated, or inferred and that, alone or in combination, personally identifies an individual student or the student's parent(s) or family.

PII, as defined by federal law, also includes 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 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.

Some examples of PII collected by CDE may include, but are not limited to, the following list:

- A student's name
- A personal identifier such as a student ID number/SASID
- Student's date of birth

- Other demographic information

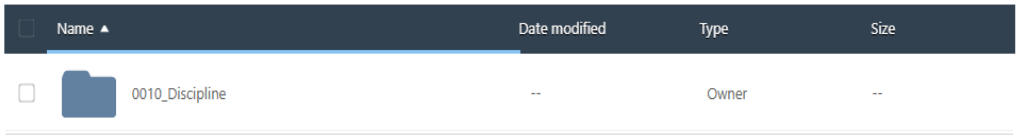
Districts should always follow local policies when distributing secure files. This information must not be emailed.

Syncplicity

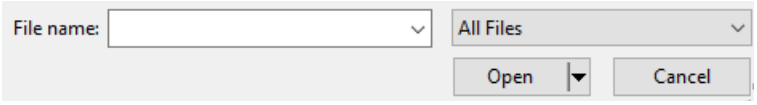
Syncplicity is an online platform used for secure file sharing. Data Respondents with the LEA Approver or LEA User role for Student Restraint and Seclusion Collection are given access to the SRS Syncplicity folder for their district by the SRS Collection lead. This folder is used whenever data respondents and the SRS collection lead need to communicate regarding sensitive student data or personally identifiable information (PII). This information must not be emailed.

Steps

1. Click here to access the Syncplicity website.
2. From the Files screen, scroll down to find your district's student folder. This folder will be named with the following naming convention: ***District Number _ SRS.***
   ***Note**: Data respondents may have multiple Syncplicity folders depending on the data collections they are responsible for or other roles where they communicate PII with CDE staff. Be sure to select the SRS folder when communicating with the SRS Collection lead because they do not have access to other folders.*



3. Click on a file to download a copy of that file to your local device or select the upload button to upload a file from your computer to Syncplicity.



4. Email the StudentRestraintSeclusion@cde.state.co.us to inform the Collection lead a document has been uploaded to Syncplicity. The Collection lead does not get an automatic notification when a file is uploaded into Syncplicity.

Section 5: SRS Data Use and Privacy Guidelines

SRS data is used primarily to report restraint data to the public and for use in the Annual Restraint Review Report . See the Mandatory Data Pipeline Collections Legislation and Uses document for more information about the legislative mandates for required CDE data.

Data Privacy Guidelines

All publicly posted data utilizes privacy guidelines. The Education Statistics Site privacy methods include blurring of cohort/membership base sizes with small populations (all students & subgroups), and limited suppression.

Individual district CEDAR/COGNOS reports available to users with SRS access in IdM do not utilize privacy guidelines to allow LEAs to review their data in complete detail.