CENTER FOR
DEMOCRACY
& TECHNOLOGY

COVID-19 AND STUDENT PRIVACY

Do’s and Don’ts for State and Local Practitioners

August 2020

Introduction to the Training Module

Welcome to the Center for Democracy & Technology's COVID-19 and Student Privacy training. The goal of this training is to equip **state and local practitioners** to navigate emerging privacy and security issues that are arising as a result of distance learning amidst the global pandemic.

In this material, we will cover:

- The importance of protecting student privacy
- Federal and state privacy legal requirements that pertain to COVID-19 and distance learning
- Steps practitioners should take to respond to unique privacy concerns related to the global pandemic
- Additional resources to protect student privacy

CDT uses Thinkific, Inc. to host this training module and use of the module is governed by Thinkific's privacy policy

IMPORTANCE OF PROTECTING STUDENT PRIVACY

What is Privacy and Why Does It Matter?

- Privacy is the idea that **people should be able to control their own information** and that the entities that are authorized to collect and use that information do so in ways that respect an individual's autonomy. In the case of education, that right refers to students and their families.

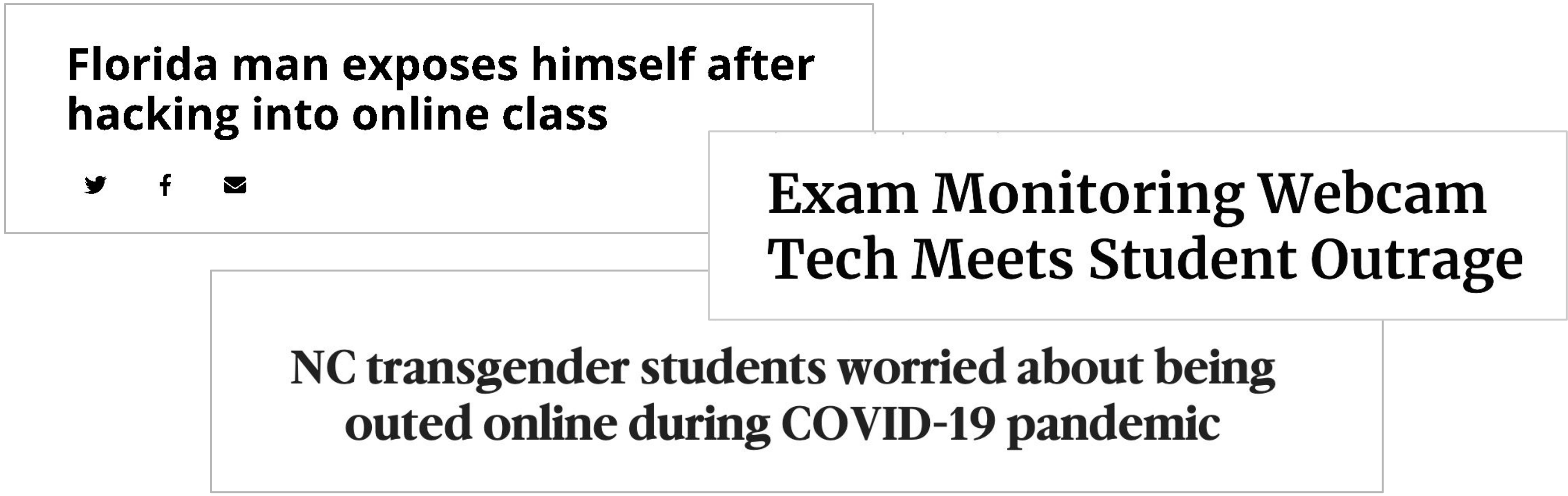
- Schools have **legal obligations** to protect students' privacy. The rules have not changed as a result of the pandemic, and every state and local education agency (LEA) has navigated them before.

- Beyond legal compliance, schools have an ethical obligation to ensure that uses of technology and data **do not come at the expense of student safety and well-being.**

COVID-19 and Student Privacy Headlines

Privacy and civil rights are often sacrificed in moments of crisis. We need to protect students online in the same way we would protect them in person.

The COVID-19 pandemic has created unique challenges for education systems, exacerbating risks to student privacy. Several incidents of compromised student privacy have attracted state and national publicity.



Florida man exposes himself after hacking into online class

Exam Monitoring Webcam Tech Meets Student Outrage

NC transgender students worried about being outed online during COVID-19 pandemic

"Florida man exposes himself after hacking into online class." - ClickOrlando.com
"NC transgender students worried about being outed online during COVID-19 pandemic." - The News & Observer
"Exam Monitoring Webcam Tech Meets Student Outrage" - Forbes

FEDERAL AND STATE LEGAL COMPLIANCE

Understanding Personally Identifiable Information (PII)

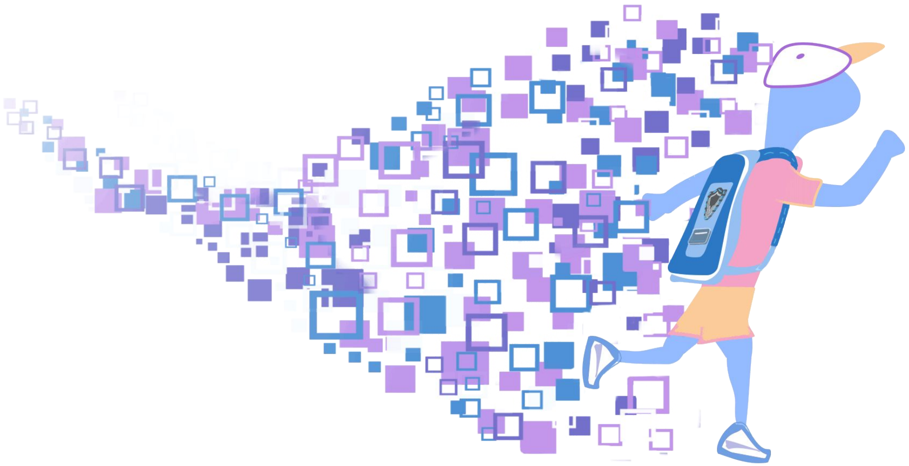
Personally identifiable information (PII) is any information that can be used to identify or distinguish a person, either directly or in combination with other information. PII is a legal concept that plays a central role in student privacy legislation.

- Personally identifiable information can be found in many different types of media, ranging from data in an education record to videos to photos to written documents.
- Common examples of PII include students' names, contact information, unique identification numbers, birthdays, places of birth, individual grades or feedback, and student health records.
- New PII elements that might be collected as a result of COVID-19 include a student's COVID-19 positivity status as well as screenshots of online classes.
- This list is not exhaustive. When protecting PII, practitioners should think critically about their specific circumstances to ensure they are not disclosing any information that can be linked to specific students.

Federal and State Student Privacy Legal Compliance

- **Federal**: At the federal level, the primary student privacy law that governs education data is the Family Educational Rights and Privacy Act (FERPA):
    - FERPA protects personally identifiable information about students.
    - FERPA generally prohibits sharing student data without parental consent but has limited exceptions.
    - The “school official exception” permits LEAs to share PII without parental consent by designating third parties as school officials if they have a legitimate educational interest, perform a service the LEA would otherwise provide, and allow the LEA to maintain direct control of student data.
- **State**: In addition to federal law, every state has introduced a bill expressly addressing the privacy and security of education data, and 45 states have collectively enacted 128 laws related to student data privacy. As state and local practitioners, you should understand the state-specific privacy laws that apply to you.

Steps to Protecting Student Privacy During COVID-19



Protecting Student Privacy During COVID-19

Data and technology resources allow states and LEAs to continue to serve students during COVID-19. To ensure these tools do not jeopardize student privacy, state and local practitioners should take the following steps:

1. Utilize existing data and technology **governance structures** and staff.
2. Provide educators with **privacy training and communications**.
3. Ensure **appropriate agreements** are in place before using new tools and products.
4. Secure **video conferencing** tools.
5. Create a legal and technical **data deletion plan**.
6. Consider **equity** throughout the use of data, technology, and privacy.

Step 1: Utilize Existing Governance Structures

What they are: According to the Institute of Education Science, data governance is "the overall management of data, including its availability, usability, integrity, quality, and security."*

- Effective governance is critical during COVID-19 to ensure that the right people are involved at the right time in decisions about data, technology, and privacy, especially when decisions are being made quickly.
- Student privacy is not a new function for state and local practitioners, so states and LEAs have previously established policies and processes to make decisions regarding privacy.

* https://nces.grads360.org/#communities/data-governance/publications/15066

Step 1: Utilize Existing Governance Structures

What you should do: Ensure that established governance structures for protecting student privacy are integrated into your COVID-19 response.

- Rely on staff that have worked on student privacy issues in the past. Individuals and working groups with past privacy experience have valuable institutional knowledge on how to navigate some of these issues.
- Incorporate privacy consideration into any new governance bodies you have created to oversee responses to COVID-19.
- Utilize existing agreements and contracts that you already have in place when expanding the use of an existing product or using a new one.

Step 2: Train and Communicate with Educators

What it is: Training and proactive communication about how to utilize new technologies while employing practices that protect privacy and keep students safe.

- Most educators do not have a background in data privacy or security, and the majority of data breaches result from human error.
- Student privacy training helps teachers understand basic technological and legal aspects of security and privacy protection, empowering them to make informed decisions.
- When making uninformed decisions regarding education technology usage, educators can jeopardize student data or even create a legal obligation for the school or district by agreeing to terms of service without proper vetting.

Step 2: Train and Communicate with Educators

What you should do: Provide training to and proactively communicate with educators about student privacy.

- Create and/or repurpose existing training to educate teachers and school administrators on their role in protecting student privacy during COVID-19.
- Offer support around video conferencing, in terms of which tool to use and the security practices needed to prevent unauthorized visitors, sharing inappropriate content, or selecting inappropriate screen names.
- Remind educators to not take screenshots and publicly post pictures of their classes and to exercise caution if classes are recorded the show students.
- Provide support and communicate around selecting learning applications and systems as educators typically lack the expertise needed to evaluate privacy policies and practices.

Step 3: Ensure Appropriate Agreements and Contracts

What they are: Written agreements that establish how an education agency will use a technology vendor's services and how that vendor will handle student data.

- Agreements and contracts have always been an important element of protecting student privacy, but are especially important as schools use new technology to navigate COVID-19.
- Written agreements help ensure that both tech vendors and education institutions understand acceptable and unacceptable uses of student data.
- Agreements with vendors are key to ensuring that local education agencies retain control over student data, a requirement under FERPA.

Step 3: Ensure Appropriate Agreements and Contracts

What you should do: Ensure appropriate agreements and contracts have been established with technology vendors prior to using new platforms or services.

- When drafting a new agreement, repurpose existing contracts with established vendors rather than drafting a new contract from scratch, even if the service is free.
  - This is particularly important for products or services that were not designed for educational purposes (e.g. video conferencing tools and social media), which may not have policies that are appropriate for student data.
- When reviewing privacy policies, pay special attention to secondary uses of student data as well as data deletion if you do not plan to use those services after schools reopen.
  - Key words like “location”, “advertising”, “third parties”, “analytics”, “share”, and “sell” may suggest data practices that do not comply with student privacy law or best practices.

Step 4: Secure Video Conferencing

What it is: Using video conferencing and recording to deliver classes is likely new for your LEA, so it important to put in place the right legal and technical requirements, especially as some video conferencing platforms were not designed for educational purposes.

- Privacy breaches related to video conferencing tools have dominated headlines as schools transition to new software. Educators can prevent many of these sorts of incidents by adjusting their tools' permissions and settings.
- Student bullying and harassment behavior is another pressing issue related to video conferencing usage. This can take the form of disruptive screen-sharing, abusive chat behavior, and offensive handles chosen for user names.

Step 4: Secure Video Conferencing

What you should do: When using video conferencing tools, follow technical and legal best practices to ensure that virtual classrooms remain a safe, productive educational space.

- Treat video conferencing as if personally identifiable information is being shared, and use appropriate agreements to ensure that you maintain direct control of the data.
- Take steps to keep out unwanted participants by setting a password and/or ensuring that the link to the meeting is long and difficult to guess.
- Restrict other users from using functionality like screensharing, recording, managing participants, or commenting in public or user-to-user chat boxes. Have a plan for managing students' speaking, presenting, and screensharing functions in light of student safety and learning goals.
- If possible, pre-assign participant names prior to the start of video calls.
- If possible, set up a process to approve participants before they can join the meeting.

Step 5: Create Data Deletion Plans

What they are: Data deletion plans determine the length of time student data is stored, either internally or by third parties, before being deleted, and the strategies used to systematically delete that data.

- Third parties that no longer have an educational purpose to retain student data are legally required to delete that data under FERPA.
- Data that is retained indefinitely can pose a threat to students and their families.
- Schools should pay particular attention to data deletion policies during COVID-19, since educators may not continue using some services once school campuses reopen.
- Moreover, schools may be using vendors that are less familiar with education contexts, so existing vendor deletion policies may not match schools' or families' expectations.

Step 5: Create Data Deletion Plans

What you should do: Create a data deletion plan for all student data.

- Make a list documenting third parties that collect student data during the COVID-19 outbreak. Set a schedule to regularly update this inventory during and after remote learning guidelines are in place.
- Use agreements and contracts to set data deletion expectations when beginning to use a new technology or service.
- Utilize best policy and technical practices when data is deleted.

Step 6: Pay Attention to Equity

What it is: Disparities in access to devices and reliable internet access as well as differing student needs require thoughtful consideration and mitigation to prevent the deepening of existing inequities.

- The emergence of COVID-19 and corresponding emphasis on education technology has exacerbated existing issues of inequity regarding device and internet access, often referred to as the "digital divide" or "homework gap."
- Students with disabilities, special education students, and English language learners are also particularly vulnerable when relying on technologies that are not equipped for their particular needs.

Step 6: Pay Attention to Equity

What you should do: Understand your students’ unique needs and tailor technology access and instructional supports to make learning as accessible as possible to all students during COVID-19.

- Assess your students’ current levels of access to devices and reliable internet access.
- Consider how your education institution can mitigate disparities in digital access. School-issued laptops, school-issued mobile hotspots, and parked buses mounted with wi-fi capabilities are all possible strategies to provide equal access to students.
- Assess your students’ unique learning needs, with a focus on students with disabilities and English language learners.

CENTER FOR DEMOCRACY & TECHNOLOGY

COVID-19 and Student Privacy

WRAP UP

Wrap Up

Thank you for participating in this training. We hope that this is helpful in providing an overview of why student privacy is so important even during a pandemic, how federal and state legal compliance factors in, and most importantly, the steps that you can take to protect student privacy during this global pandemic.

As stated before, privacy is not new in education, so there are existing resources that can and should support schools during this crisis.

Please send us feedback on how we can improve this training and feel free to reach out with additional questions.

Student Privacy Resources

- **State student privacy laws:** The Data Quality Campaign and FERPA Sherpa both offer online resources summarizing and comparing state student privacy laws
https://ferpasherpa.org/state-laws/
https://dataqualitycampaign.org/education-data-legislation-review/
- **Governance:** The Department of Education discusses best practices for educational data governance in a report:
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data_Governance_and_Stewardship_0.pdf
- **Contracts**: The Student Data Privacy Consortium works with state and local education agencies to create model contracts:
https://privacy.a4l.org/
- **Training:** iKeepSafe provides a series of educator training modules on data privacy in education, available online for free:
https://ikeepsafe.org/data-privacy-in-education-an-ikeepsafe-educator-training-course/
- **Video conferencing**: The Consortium on School Networking released a toolkit on technical best practices for securing video conferencing tools:
https://www.cosn.org/sites/default/files/Member%20Brief%20-%20Video%20Conferencing%20040120.pdf

Student Privacy Resources

- **Privacy policies**: Common Sense Media has reviewed and evaluated privacy policies: https://privacy.commonsense.org/
- **Deletion**: CDT has issued guidance on best practices around data retention and deletion: https://cdt.org/insights/report-balancing-the-scale-of-student-data-deletion-and-retention-in-education/
- **FERPA and COVID-19**: The U.S. Department of Education released guidance on navigating privacy questions related to COVID-19 and FERPA: https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19
- **FERPA and virtual learning**: The U.S. Department of Education hosted a webinar and posted slides: https://studentprivacy.ed.gov/training/ferpa-and-virtual-learning-during-covid-19-webinar-recording https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAandVirtualLearning.pdf

Student Privacy Resources

- **Equity**: Learning Keeps Going and Educating All Learners are two organizations that provide resource libraries addressing education equity issues.
  - https://www.learningkeepsgoing.org/
  - https://www.educatingalllearners.org/
- **Working with parents**: CDT also released a guide for parents on navigating student privacy issues:
  https://cdt.org/insights/a-parents-guide-to-student-privacy/

COVID-19 and Student Privacy

CDT'S VISION

PUTTING DEMOCRACY AND INDIVIDUAL RIGHTS AT THE CENTER OF THE DIGITAL REVOLUTION

CDT's Student Privacy Project

- *Provide **balanced advocacy** that promotes the responsible use of data and technology while protecting the privacy rights of students and their families.*
- *Create **solutions-oriented policy resources** that are grounded in the problems that currently confront education practitioners and technology providers who work with them.*
- *Offer **technical guidance** that can be adapted and implemented by education practitioners and the technology providers who support them.*

Contact Us

Student Privacy Project
Center for Democracy & Technology
StudentPrivacy@cdt.org