CENTER FOR DEMOCRACY & TECHNOLOGY

Privacy and Equity in the New School Year

Steps for In-Person, Remote, or Hybrid Learning

November 2020

Introduction to the Training Module

Welcome to the Center for Democracy & Technology's module on Privacy and Equity in the New School Year. The goal of this training is to equip **state and local practitioners such as school administrators and teachers** to navigate emerging privacy and security issues for learning either in-person or remotely.

In this material, we will cover:

- The importance of protecting student privacy
- Emerging **in-person** privacy practices
- Emerging **technology-based** privacy practices

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 must do so in ways that respect the individual's autonomy and avoid doing harm to the affected people. 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 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.**

Student Privacy Headlines

Privacy and civil rights are often challenged in moments of crisis or transition, and the return to schools during a pandemic is no exception.

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

Covid in the Classroom? Some Schools Are Keeping It Quiet

The dystopian tech that companies are selling to help schools reopen sooner

L.A. schools announce massive COVID-19 testing, tracing initiative for all students and staff

EDUCATION NEWS

Remote learning can give a window into students' home lives — whether they want it or not

[Covid in the Classroom? Some Schools Are Keeping It Quiet - NY Times]
[The dystopian tech that companies are selling to help schools reopen sooner - Vox]
[L.A. schools announce massive COVID-19 testing, tracing initiative for all students and staff - LA Times]
[Remote learning can give a window into students' home lives - Daily Press]

Schools' Approaches to Reopening

Schools have adopted three models for reopening this fall:

- **Socially distanced in-person learning:** In-person learning in the COVID context looks quite different from what schools were doing before the pandemic. It has required numerous interventions to make in-person schooling sufficiently safe, such as providing necessary safety resources like hand sanitizer, reducing class sizes, restricting activities to those that allow for social distancing, and reorganizing mealtimes to minimize group gathering and sharing of spaces.

- **Remote learning:** Continued remote learning is another approach to limit the spread of the coronavirus. While there are non-technical approaches such as providing paper worksheets at pick-up points for students, many remote learning approaches rely on technology such as laptops or tablets, reliable internet, and videoconferencing. These tech-based approaches may present substantial equity and privacy concerns, such as access to broadband or sufficient devices and the collection of student data.

- **Hybrid learning:** A hybrid model combines both in-person and remote learning, either by having students come to school in person in "shifts" and learn remotely during other periods, or by livestreaming classes so they are available to students both in-person and remotely.

EMERGING IN-PERSON PRIVACY PRACTICES

Emerging In-Person Privacy Practices

Collecting data related to the well-being of students is a long-standing, common duty of educational institutions, and schools returning to in-person learning are collecting **new types of data** for a variety of purposes:

- In order to prevent and mitigate the spread of COVID-19, school reopening plans are turning to approaches like collecting information to assist health agencies in **contact tracing** and widespread **testing**.
- Others are thinking about how to make schools stronger and more equitable in the aftermath of COVID-19 by better **understanding the inequities faced by students** that were exacerbated by the COVID-19 crisis, and how to ensure both the physical and emotional health of their students upon reopening.

Emerging In-Person Privacy Practices

While these are important goals, they often entail collection of sensitive data, so it is important to consider the privacy and equity concerns they raise. Privacy risks might come in the form of:

- **Overcollection:** While it may feel like the best thing to do is collect as much information about students' health and movements as possible, in case it becomes useful later, this approach is dangerous from a privacy perspective. The more data that is collected on students, the more risk there is for that data to be accidentally exposed or misused in a way that is harmful to the student.

- **Breaches and redisclosure:** Any time data are collected, there is a risk that it could be breached or redisclosed. Marginalized groups of students like transgender students, students experiencing homelessness, and students with disabilities are more at risk if their health information is disclosed or misused, as exposure of this information can lead to bullying, feelings of alienation, and discrimination.

Emerging In-Person Privacy Practices

Privacy risks might come in the form of:

- **Inadvertently disclosing private information:** When collecting and handling sensitive data, there is often a risk that that sensitive information will be exposed, even when the underlying data are used properly. For instance, if a contact tracer notifies all students in a class that they may have been exposed to the coronavirus, and the next day one class member switches to remote learning, the now-remote student's health information has been exposed.
- **Stigmatization:** Related to revealing information is the concern that students may be stigmatized for their health status. If a student is revealed to have contracted COVID, their classmates or other parents may hold that student responsible or ostracize the student out of a sense of fear, even if they are no longer contagious.
- **Legal risk for the school:** Schools opting to collect and share data with local health agencies face some legal risk, as federal and state privacy law can be confusing and may not necessarily permit data sharing.

Emerging In-Person Privacy Practices

As described in the next slides, schools can take the following steps:

- **Consider equity and engage the community**: Schools should involve students, families, and teachers in planning, implementing, and eventually ending data collection and sharing programs.
- **Comply with federal and state law**: Schools should collect and share student health information only as permitted by the Family Educational Rights and Privacy Act (FERPA), other federal laws, and state law.
- **Establish formal structures for data governance**: Schools should also develop robust data governance practices and policies, which give faculty and staff the tools to manage student data in a consistent and appropriate way.

Emerging In-Person Privacy Practices

Equity and Community Engagement

Community engagement means involving students, families, and teachers in planning, implementing, and ending data collection and sharing programs. In engaging the community, schools should:

- Be transparent, alerting families and other stakeholders to both the benefits and risks associated with the program.
- Apprise the community of the goals of the program, the data being collected, the uses of the data, and the community's rights to review, amend, or delete collected information, or possibly opt out of the collection entirely.
- Accommodate parents and guardians who may work multiple jobs or evening and night shifts, speak a language other than English, have a disability, or lack access to transportation or broadband internet.

Emerging In-Person Privacy Practices

Legal Compliance - Overview

Legal compliance means collecting, using, and sharing student data as required or limited by **federal** and **state** law.

- **Federal**: At the federal level, the primary student privacy law is the Family Educational Rights and Privacy Act (FERPA):
  - FERPA protects **personally identifiable information** (PII) from **education records.**
    - PII is any information that can be used to identify or distinguish a person, either directly or in combination with other information.
    - Examples of PII include students' names, contact information, identification numbers, birthdays, places of birth, individual grades, and health records.
  - FERPA generally prohibits sharing student data without parental consent but has limited exceptions, including a **health and safety emergency exception**.
- **State**: Every state has introduced a bill expressly addressing the privacy and security of education data. As state and local practitioners, you should understand the state-specific privacy laws that apply to you.

Emerging In-Person Privacy Practices

Legal Compliance - Sharing Data

Schools collecting and sharing health information may comply with the FERPA by:

- Sharing information as permitted by FERPA's **health and safety emergency** exception.
- Partnering with **independent health clinics**, which do not receive funding from the U.S. Department of Education and are not subject to FERPA, to collect and maintain student health data related to COVID-19.
- Disclosing only **deidentified data**, which has had all PII removed.

We will explore each of these options on the next slides.

Emerging In-Person Privacy Practices

Legal Compliance - Sharing Data

FERPA's **health and safety emergency exception** may allow schools to share PII without parental consent if certain requirements are met.

- The health and safety emergency exception may apply if:
  - Information is disclosed to "**appropriate parties,**" such as health agencies or medical professionals
  - To "**protect the health or safety** of the student or other individuals"
  - From "an **articulable and significant threat** to the health or safety of a student or other individuals" as determined by school officials.
- The exception is "**temporally limited** to the period of the emergency and generally does not allow for a **blanket release** of personally identifiable information."
- During the H1N1 pandemic, the U.S. Department of Education advised that the exception could apply, "so long as there is a **current outbreak** of H1N1 in the particular school or school district."

Emerging In-Person Privacy Practices

Legal Compliance - Sharing Data

- Student health data may also be shared if schools enlist **independent health clinics** to collect and maintain student data related to COVID-19. FERPA applies only to education records "maintained" by or on behalf of "an educational agency or institution" that has received funds from the U.S. Department of Education, and independent health clinics usually do not receive U.S. Department of Education funding. Note that any student health data shared by the independent health clinic with the school will likely be covered by FERPA.

- A school may share **de-identified** student information with a health agency.

    - De-identified data has had "enough personally identifiable information removed or obscured so that the remaining information does not identify an individual and there is **no reasonable basis** to believe that the information can be used to identify an individual."

    - Techniques to de-identify information include presenting it in **aggregate form** or redacting personal information. De-identification, however, must avoid students being re-identifiable, including because small groups appear in aggregate data or in light of "other reasonably available information."

Emerging In-Person Privacy Practices

Data Governance

In addition to engaging the community and ensuring that data collection practices meet legal requirements, schools should also develop robust **data governance practices** and **policies**. Data governance means the school policies that, along with the training that accompanies them, give faculty and staff **tools to manage student data in a consistent and appropriate way**. There are a number of elements that should be incorporated into governance for COVID-related data:

- **Data governance structures:** Establish a formal data governance structure for making decisions about COVID-related data, ensuring that all the necessary voices are heard for each decision, and resolving any confusion or conflicts about those decisions. This structure should be a continuation of the community engagement process.

- **Goals for data collection:** Set explicit goals for COVID-related data collection to evaluate the efficacy of the program and determine if the program needs to be adjusted and when it should be discontinued. These goals and metrics should also be communicated with the community.

Emerging In-Person Privacy Practices

Data Governance

- **Access, use, and redisclosure limitations:** Ensure that there are use limitations attached to shared data, such as restrictions on publication, resharing, or reuse. These limitations should be codified in data sharing agreements with other agencies to ensure the data are used as expected.
- **Retention and deletion plans:** Determine when and how data will be deleted. This may be an explicit timeline, such as two weeks after the end of the school year, or may be defined by conditions that must be met, such as the development of a vaccine.
- **Storage and transfer:** Choose secure methods for securing and storing data. Where and when possible, data should be encrypted, and all data should be accessible only to those who need that access to do their jobs. Insecure methods for transferring data, like email or fax, are susceptible to interception, and so do not provide enough protection for sensitive student information.

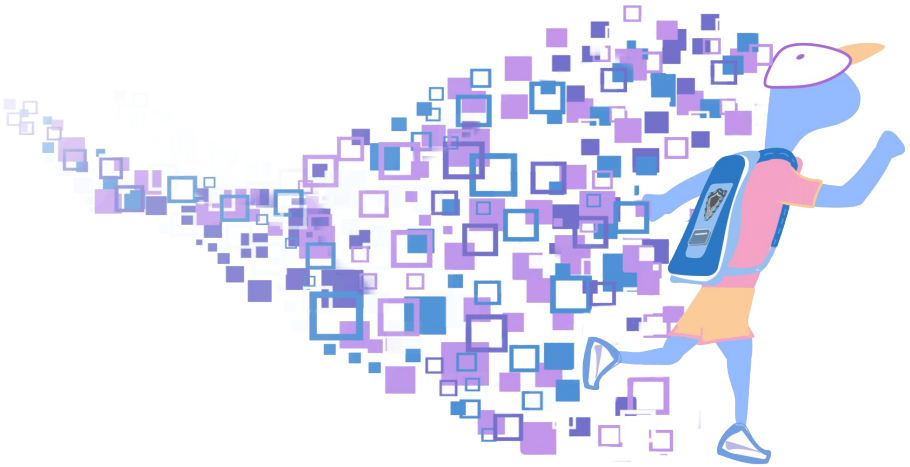
Emerging In-Person Privacy Practices

Data Governance

- **Security and breach responses:** Ensure that data breach plans account for new COVID-related data. There should be clear roles for the school and any other agency who may have access to the data, including plans to communicate with families so they know if they were affected and where to go for further assistance.

- **Data sharing agreements:** Enter into a written data sharing agreement with health agency partners. In drafting those agreements, the school and health agency should detail the type of information being collected, the method and purposes of the collection, permitted uses of the information, and retention and destruction requirements (including a timeline for doing so). Agreements should also include limitations on access to and redisclosure of the information, administrative and technical measures to ensure security and prevent unauthorized access or uses, and the school's right to conduct audits. The provisions of a data sharing agreement should comply with state and federal law; as noted above, data shared with a school by an independent health clinic will likely be covered by FERPA.

EMERGING TECHNOLOGY-BASED PRIVACY PRACTICES



Emerging Technology-Based Privacy Practices

Many school districts have adopted new technology to help students continue learning in the face of the pandemic. Tech-based approaches to remote learning may allow for a higher level of engagement between teachers and students than other options such as paper packets, and may allow teachers to gather data to better understand effective teaching practices.

As with any time schools use new technology, it is important to do so in a way that respects the privacy, safety, and well-being of students and their families. There are a range of risk factors that could apply to technology that was adopted during the pandemic, including:

- The technology may not have been designed for an educational context, and consequently may not be adapted for the issues and legal framework that schools present.
- Education technology (EdTech) adopted for remote learning may not have gone through schools' and districts' normal governance procedures. Unvetted technology could expose information in unexpected ways and may introduce access and equity concerns if it does not include necessary accessibility features, or is incompatible with adaptive technology used by students or teachers.

Emerging Technology-Based Privacy Practices

To address risk factors that apply to technology that was adopted during the pandemic and take advantage of its benefits, schools should:

- **Inventory EdTech:** Build an accurate picture of all the technology currently in use in the school, including by individual teachers. After inventorying systems, there are two approaches to managing the new technology: incorporating the technology, or responsibly decommissioning it.
- **Incorporate new technology:** Ensure that new technology meets legal requirements, can adhere to internal governance policies, and is compatible with other technology used by the school.
- **Decommission new technology:** Download any information teachers will need in the future from any EdTech the school does not wish to keep using and take steps to ensure that information is deleted from the system.

Emerging Technology-Based Privacy Practices

Inventory EdTech

- Engage with teachers to inventory what, if any, technology they have adopted during remote learning
- Create an open process, not a punitive one, to ensure that teachers feel comfortable being forthcoming
- Take an expansive view of technology: everything from streaming lessons on Facebook Live to learning management systems
- Continue the inventory process in the future, accounting for new technology as it is added to adapt to schools' changing needs

Emerging Technology-Based Privacy Practices

Incorporate New Technology

After completing the inventory process, any technology the school wishes to retain should be incorporated into existing systems:

- Ensure legal compliance with federal and state law.
- Review agreements with the EdTech vendor for compliance with internal data governance policies, such as whether:
    - The new technology requires obtaining parental consent for student use.
    - The technology can adhere to schools' requirements about how that data are used by third parties.
    - Any configurations need to be set to ensure the technology performs appropriately, and the data are handled as expected.
- Ensure that the new technology is compatible with existing systems such as a student information system, learning management system, or system for maintaining files of students' work so that data from the new technology may be readily used by teachers and administrators.

Emerging Technology-Based Privacy Practices

Decommission New Technology

If the school does not wish to keep using the new EdTech, it must responsibly decommission it by taking the following steps:

- Download information such as student assignments, grades, or attendance lists from the technology for future use in a format that is compatible with existing systems.
- As necessary, save copies of student work.
- Notify students, families, and staff of the decommissioning.
- Delete the data, which may require more than simply disabling the teacher account. The tool's terms of service may provide more information about how to truly delete user data. If not, schools may also need to consult with their legal and information technology departments to explore next steps.

WRAP UP

Wrap Up

Thank you for participating in this training. We hope that this is helpful in providing an overview of the steps that you can take to protect student privacy as the new school year begins. This training was based on our report "Privacy and Equity in the New School Year," which can be found at:
https://cdt.org/insights/report-privacy-and-equity-in-the-new-school-year/

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

Student Privacy Resources

Best Practices

- Center for Democracy & Technology, *COVID-19 and Student Privacy: Do's and Don'ts for State and Local Practitioners* (Sept. 1, 2020), https://cdt.org/insights/covid-19-and-student-privacy-dos-and-donts-for-state-and-local-practitioners/
- Hannah Quay-de la Vallee & Cody Venzke, Center for Democracy & Technology, *Privacy and Equity in the New School Year* (July 26, 2020), https://cdt.org/insights/report-privacy-and-equity-in-the-new-school-year/
- Hugh Grant Chapman & Cody Venzke, Center for Democracy & Technology, *Student Privacy and Learning Pods: New Education Models in a Pandemic* (Nov. 13, 2020), https://cdt.org/insights/student-privacy-and-learning-pods-new-education-models-in-a-pandemic/

Legal Compliance

- U.S. Department of Health and Human Services & U.S. Department of Education, *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records* (Dec. 2019), https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records
- Centers for Disease Control and Prevention, *Health Information & Privacy* (Sept. 14, 2018), https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html

Student Privacy Resources

Legal Compliance (cont'd)

- Student Privacy Policy Office, *FERPA & Coronavirus Disease 2019 (COVID-19)* (Mar. 2019), https://studentprivacy.ed.gov/resources/ferpa-and-coronavirus-disease-2019-covid-19
- Privacy Technical Assistance Center, *FERPA Exceptions Summary* (Apr. 2014), https://studentprivacy.ed.gov/resources/ferpa-exceptions-summary-apr-2014-2-page-standard-size

Data Deletion and De-Identification

- Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Protecting Privacy While Supporting Students Who Change Schools* (June 20, 2019), https://cdt.org/insights/protecting-privacy-while-supporting-students-who-change-schools/
- Elizabeth Laird & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Balancing the Scale of Student Data Deletion and Retention in Education* (Mar. 2019), https://cdt.org/insights/report-balancing-the-scale-of-student-data-deletion-and-retention-in-education/
- Marilyn Seastrom, National Center for Education Statistics, *Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records* (Nov. 23, 2010), https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601
- Privacy Technical Assistance Center, *Data De-identification: An Overview of Basic Terms* (May 2013), https://studentprivacy.ed.gov/resources/data-de-identification-overview-basic-terms

Student Privacy Resources

Data Governance and Written Agreements

- Privacy Technical Assistance Center, *Guidance for Reasonable Methods and Written Agreements* (Aug. 2015), https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements
- Privacy Technical Assistance Center, *Written Agreement Checklist* (July 2015), https://studentprivacy.ed.gov/resources/written-agreement-checklist
- Privacy Technical Assistance Center, *Data Governance Checklist* (Dec. 2011), https://nces.ed.gov/Forum/pdf/data_governance_checklist.pdf

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