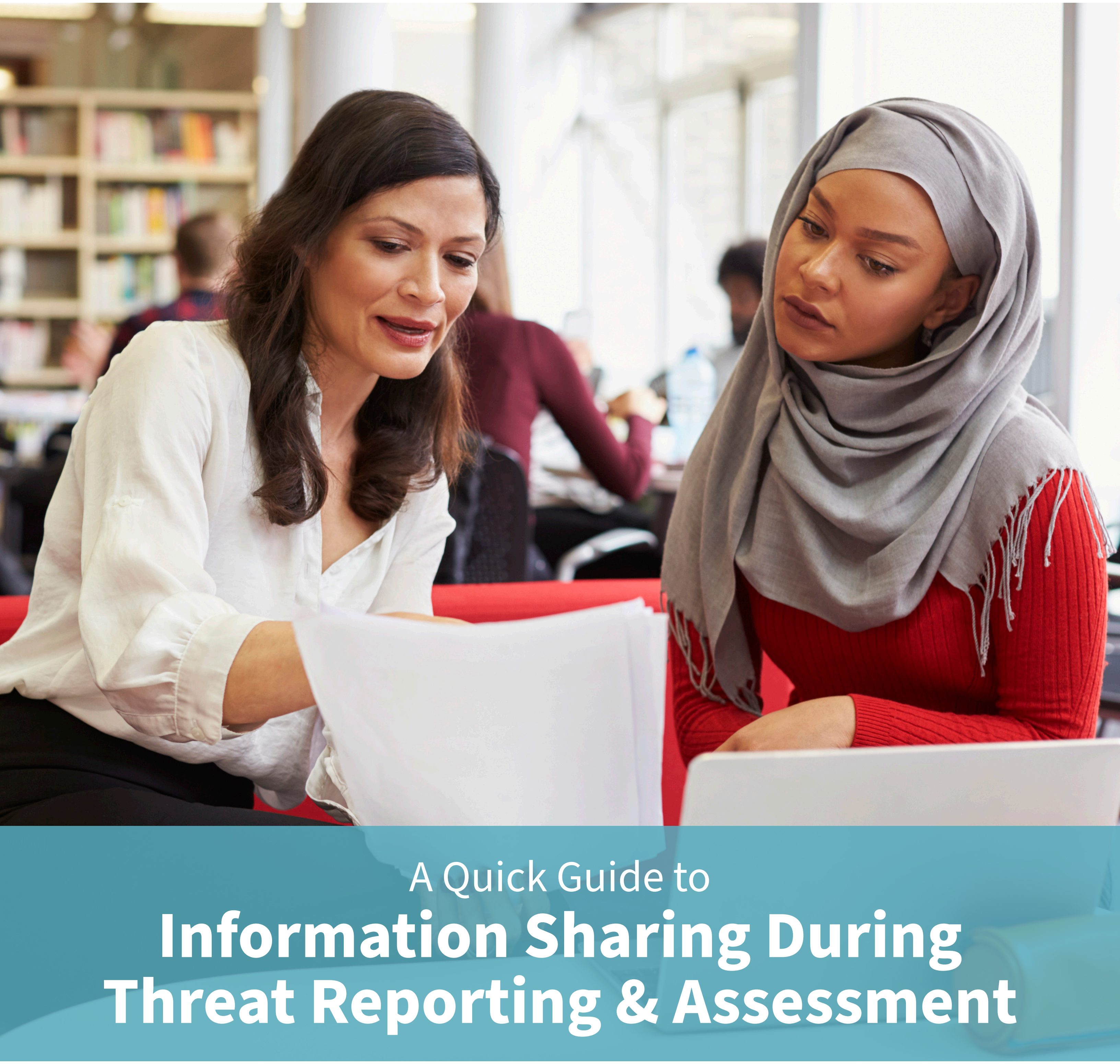
National Center for School Safety



A Quick Guide to

# Information Sharing During Threat Reporting & Assessment

SCHOOL OF
PUBLIC HEALTH
UNIVERSITY OF MICHIGAN

## Contributors

Allison Schreiber, MAIR
School Safety Specialist
National Center for School Safety

Aysha Lonich, MEd, BCBA
School Safety Specialist
National Center for School Safety

Brent Allen Miller, MA, PMP
Training Manager
National Center for School Safety

Heather Murphy, MA, LPC, NCC
School Safety Specialist
National Center for School Safety

Kiera Dressler, MSW Candidate
Research Assistant
National Center for School Safety

Sarah Mason, MPH Candidate
Research Assistant
National Center for School Safety

## About the National Center for School Safety

The National Center for School Safety (NCSS) is a Bureau of Justice Assistance-funded training and technical assistance center at the University of Michigan School of Public Health. As a multidisciplinary, multi-institutional center focused on improving school safety and preventing school violence, the NCSS team is composed of national leaders in criminal justice, education, social work, and public health with expertise in school safety research and practice. NCSS provides comprehensive and accessible support to Students, Teachers, and Officers Preventing (STOP) School Violence grantees and the school safety community nationwide to address today's school safety challenges. NCSS serves as the national training and technical assistance provider for the STOP School Violence Program.

### Funding Disclaimer

This project was supported by Cooperative Agreement No. 2019-YS-BX-K001 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics; the National Institute of Justice; the office of Juvenile Justice and Delinquency Prevention; the Office of Victims of Crime; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.  Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S Department of Justice.

National Center
for School Safety
University of Michigan
School of Public Health
1415 Washington Heights
Ann Arbor, Michigan 48104
nc2s.org

Published July, 2022

## About this Guide

### Who is This Quick Guide For?

This document is for principals, teachers, school administrators, school resource officers, school counselors, threat assessment teams, and mental health providers.

### What is the Purpose of This Quick Guide?

Schools rely on sharing data, and student information is often provided to others outside the school or district. Under the Family Educational Rights and Privacy Act (FERPA), personally identifiable information from education records cannot be disclosed without written consent; however, FERPA includes exceptions that permit data sharing under certain conditions.[1]

This document brings together resources that explain when to release or withhold student information collected through reporting systems and threat assessment processes.

## Contents

# Information Sharing Overview

## Why is Information Sharing Important?

Sharing information should never be used to profile or discriminate, but rather to prevent incidents and protect students, staff, and the community. Information sharing is a crucial part of any school system because it allows transparency among staff and encourages teamwork to achieve positive results. It is also a key part of behavioral threat assessment and management (BTAM), and ensuring school safety.

Information sharing can occur internally within the school system or externally to law enforcement, family members, mental health providers, and/or community organizations. Both internal and external communication are subject to strict laws and regulations in order to protect student privacy and ensure the most positive outcome for students and staff.

## What Information Can Be Shared?

***Directory Information:*** This is defined as information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, phone number, club involvement, etc. This information can be disclosed without express written permission as long as parents/students are made aware of what is considered "directory information" and given an opportunity to opt out (typically at the beginning of each year).[2] Information can also be disclosed in the event of a health or safety emergency.[3]

## What Information Cannot Be Shared?

All other personally identifiable information from an educational record is protected by law in the United States. FERPA defines education records as "records that are: (1) directly related to a student and (2) maintained by an educational agency or institution or by a party acting for the agency or institution."[4]

The following table provides examples of records that are generally considered or not considered to be education records:[5],[6]

| **Education Records**<br>***protected under FERPA*** | **Not Education Records**<br>***not protected under FERPA*** |
|---|---|
| Transcripts | Records that are kept in the sole possession of the maker and used only as personal memory aids |
| Disciplinary records | Law enforcement unit records |
| Standardized test results | Grades on peer-graded papers before they are collected and recorded by a teacher |
| Health and family history records | Records created or received by a school after an individual is no longer in attendance and that are not directly related to the individual's attendance at the school |
| Records on services provided to students under the Individuals with Disabilities Education Act (IDEA) | Employee records that relate exclusively to an individual in that individual's capacity as an employee |
| Records on services and accommodations provided to students under Section 504 of the Rehabilitation Act of 1973 and Title II of the Americans with Disabilities Act (ADA) | Information obtained from a school official's personal knowledge/observation |

# Revelant Laws

## What is the Purpose of FERPA and HIPAA? How Do They Relate?

The Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) are two federal laws put in place to protect the privacy of an individual's personal records. FERPA refers specifically to educational records while HIPAA refers to medical records. Generally, HIPAA does not apply to schools because they are not HIPAA covered entities, but in some situations a school can be a covered entity if healthcare services are provided to students. If schools collect student health information that is contained in student education records, that information is covered by FERPA and is exempt from HIPAA.[7]

While both laws prohibit the sharing of an individual's personal records without their consent, there are exceptions permitted in certain circumstances. Guides to each law are available at the links below:

- FERPA: A Guide for First Responders and Law Enforcement
- FERPA Exceptions—Summary
- HIPAA Privacy Rule: A Guide for Law Enforcement

### When Can I Share Protected Information?

According to FERPA, exceptions can be made to allow information sharing with outside entities (such as law enforcement, local educational agencies, etc.) in certain situations, including:[8]

- Sharing during articulable and significant **health and/or safety emergencies** (in an emergency, disclosures can be made to any party—law enforcement, public health, medical officials, and parents of an eligible student—whose knowledge of the information is necessary to protect the health or safety of the student or other individuals)
- When the information being shared has **no personally identifiable information** (such as the student's name, names of family members, social security numbers, etc.)
- When a student or parent (if the student is under 18) provides **written consent** that is signed, dated, and specifies the records that may be disclosed, the purpose of the disclosure, and identification of to whom the disclosure may be made
- When information is personally known or observed (including notes, drawings, and pictures) and **not part of any educational record** (i.e., records that are directly related to a student and maintained by an educational agency/institution, or by a party acting for them)
- Compliance with **Judicial Orders** or lawfully issued subpoenas
- Sharing to other school officials (coaches, teachers, school resource officers, etc.) with **legitimate educational interest**

## What About Professional Reporting Mandates?

Many states have specific laws requiring educational staff to be mandated reporters. These laws allow an exception to FERPA in order for staff to communicate with Child Protective Services and/or law enforcement.

Exact expectations and regulations vary so make sure to check with your state and school district.

One example of how FERPA and professional reporting mandates interact in Michigan can be found in the Confidentiality of Educational Records and Child Protective Proceedings.

## What About Virtual Learning?

The COVID-19 Pandemic and resulting transition to virtual learning have created questions regarding student privacy and confidential communication. While each state and school district handles virtual learning uniquely, the U.S. Department of Education has released many resources addressing FERPA in a virtual learning environment.[9] Highlights and links to additional resources are below:

- FERPA allows teachers to take students' education records home; however, they are prohibited from disclosing the personally identifying information from the education records, except as otherwise permitted under FERPA, and should use reasonable methods to protect the education records.
- HIPAA does have Privacy and Security restrictions but waivers can be issued in times of a declared emergency. Notices issued during the COVID-19 public health emergency identified some apps that are compliant with the HIPAA standard and may be used for telehealth services, including sharing of medical information.
- The staff members need to recognize the inherent risk of background observers in a virtual setting. During lessons and discussions, staff members must avoid disclosing any form of personal identifying information that is protected by FERPA.
- Additionally, school personnel need to be aware of background observers in their environment and take care not to disclose a student's personal identifying information within earshot of their spouse, roommate, etc.
- Recording of virtual lessons and sharing is permitted under FERPA, assuming no personal identifying information was shared.

This collection of FERPA and Virtual Learning Related Resources released by the U.S. Department of Education Student Privacy Policy Office in March 2020 provides further information on best practices and policies.[10]

## Does FERPA Apply to Family Members, Staff, or Students From Another School?

FERPA applies specifically to education records, so anything disclosed by a family or staff member is not protected by FERPA and can be shared with law enforcement, school administrators, etc. However, professional discretion is expected of members of the school community.

If the information shared involves a student from another school, it is protected by FERPA. However, school officials can share that information with school officials from another school as long as it falls under one of the previously listed exceptions to FERPA (personally observed, health or safety emergency, legitimate educational interest, etc.).

Additionally, if a student transfers to another school and an active management plan is in place, or if there remains a moderate to a high level of concern regarding safety, a threat assessment team may notify the new school of the situation.

### How Do Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act Fit In?

Behavioral threat assessment and management (BTAM) and individualized education program (IEP) teams must work together to ensure student's rights and specific needs are balanced with school safety. Students' legal rights and protections afforded through the Individuals with Disabilities Education Act (IDEA) or Section 504 will remain in place and should be taken into consideration throughout the BTAM process. BTAM teams must operate with an understanding of the impact that IDEA regulations have on decisions made during the threat assessment process for students with disabilities. These regulations include:[11]

- Safeguards to ensure special education procedures are followed
- Processes to assess the function of a behavior and establish supports (functional behavioral assessment, behavior intervention plan)
- Procedures for disciplinary removals (if less than 10 days or more than 10 days) and interim alternative educational placement (45-day rule)
- Manifestation determination reviews (MDRs): If a decision is made to change the placement of a child with a disability because of a violation of the code of student conduct, a review of the child's IEP, teacher observations, and any relevant information provided by the parents must be conducted within 10 school days to determine whether the conduct was caused by, or had a direct and substantial relationship to, the child's disability; or whether the conduct in question was the direct result of the local education agency's failure to implement the IEP[12]
- Procedures for change in placement or programming, which may include adjustments to the IEP or behavior plan
- Parent notification, consent, appeals/due process
- Access to records (FERPA)

For additional information on Section 504 and the education of students with disabilities, refer to the U.S. Department of Education's "Protecting Students With Disabilities" webpage.[13]

### How Do Disabilities Influence BTAM?

Threat assessment processes help determine if threats are valid and legitimate while considering if or how a student's disability may affect the validity of a threat. Threat assessment teams should include an individual with special education expertise, a counselor, and/or a social worker to provide necessary context regarding concerning behavior.

Students with a disability may be reported to threat assessment teams for safety concerns regarding self (suicidality, hopelessness, sudden change in behavior/appearance). The special education team can create or adapt a management plan to connect the student to appropriate supports and resources while provide necessary accommodations and environmental changes. It is critical to provide staff training on antecede strategies, how to teach skills and prosocial behaviors, how to respond to challenging behaviors, and how to de-escalate situations.

## Best Practices

### How Should I Share Information?

FERPA does not specifically address the use of any application or web service; however, when deciding what virtual platform and communication service to use, schools and school districts should work with their information security officers and attorneys to review information security requirements and terms of service thoroughly. It may be helpful to consult with an attorney on threat assessment cases if there are concerns regarding information sharing.

Schools and districts will have to consider the use of online educational services on an individual basis to determine if disclosure of FERPA-protected information is required. And if it is, schools must ensure that FERPA requirements are met, in addition to any other applicable state, tribal, or local laws, and that written consent is received from the parent (if the student is under 18 years old) and/or student.[14]

### How Should I Obtain Written Consent From Families?

When obtaining written consent from families, it is important to be as transparent as possible. This includes specifying what information will be released, to whom, for what purpose, and when. It is also important to specify if this is a one-time release of information or an ongoing open line of communication.[15]

Refer to the FERPA Model Notification of Rights for Elementary & Secondary Schools document as an example.

## How Does Information From Anonymous Reporting Systems Fit In?

When partnering with an anonymous reporting system vendor, it is essential to ensure that they agree to comply with FERPA and any state, local, or tribal student data privacy statutes. Without an agreement, the board of education could be held liable for violating FERPA and/or other data privacy laws.[16]

## Final Note

It is important to remember that FERPA should serve as the baseline expectation for schools, but it is highly encouraged that schools take further necessary measures to ensure student privacy is maintained and respected.

# Additional Resources

**11.0 FERPA and HIPAA: What Threat Assessment Teams Need to Know, Texas School Safety Center**
This guide helps threat assessment teams understand how to balance the safety of the school with the privacy of individual students.

**Best Practices for Online Educational Systems, U.S. Department of Education**
This document features   and best practices for the protection of student privacy when utilizing virtual platforms for educational and administrative purposes.

**A Global Unified Message Regarding Information Sharing, U.S. Department of Justice**
This two-page resource provides guidance on planning for system interoperability, incorporating nationwide information sharing programs into policies and plans to leverage existing trusted information sharing platforms, and applying best practices to improve access to data while ensuring privacy, civil rights, and civil liberties protection and data security.

**Information Sharing Guide for K-12 Public Schools, Virginia Department of Criminal Justice Services**
This guide is a resource for school and law enforcement personnel to help them identify issues for discussion with their legal counsel when considering how they can share pertinent student information effectively.

**Mapping Data Flows, U.S. Department of Education**
This is a suggested activity for school officials to complete in order to pinpoint any potential challenges or areas for improvement.

**The Principal's Guide to Understanding FERPA, Fordham University School of Law**
This guide provides answers to common questions that principals may have, such as:

- What are special circumstances for the disclosure of education records?
- What are my specific duties under FERPA?
- How can I ensure my school is FERPA-compliant?

**Privacy and Data Sharing, U.S. Department of Education**
The resources on this webpage address the topic of data sharing and are intended to provide best practices and legal requirements for protecting student privacy while sharing data between educational agencies and partner organizations.

**Protecting Student Privacy for K-12 School Officials, U.S. Department of Education**
This is an extensive collection of resources from webinars and case studies to flyers and handouts on FERPA rights and regulations for a wide variety of situations that may occur in a K-12 school system.

**School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA), U.S. Department of Education**
This resource is comprised of information for School Resource Officers, but it is valuable for any member of the school community. It breaks down the explanation of FERPA into an easy to understand FAQ format.

**The Teacher's Guide to Understanding FERPA, Fordham University School of Law**
This resource provides guidance and resources to help teachers better understand FERPA. It also provides advice on how to deal with technology use during lessons, keeping student data secure, and responding to access requests. The guide walks through responses to several scenarios to help teachers understand the ins and outs of FERPA; for example: "You leave your room for a few minutes during your planning time. Before you left you were working with personal student information but you did not lock your computer. While you were gone, an unauthorized person came by your room and retrieved some student information from the computer screen. Under FERPA, is your school responsible?"

# References

[1]. FERPA Exceptions—Summary. (2014). Privacy Technical Assistance Center (PTAC). https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf

[2]. U.S Department of Education, Privacy Technical Assistance Center. (2019). School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA). 22.

[3]. Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. § 99.36 (1974).

[4]. FAQ 518 Does FERPA or HIPAA apply to records on students at health clinics run by postsecondary institutions? | Guidance Portal. (n.d.). Retrieved January 27, 2022, from https://www.hhs.gov/guidance/document/faq-518-does-ferpa-or-hipaa-apply-records-students-health-clinics-run-postsecondary

[5]. Information Sharing: Family Educational Rights and Privacy Act (FERPA). (n.d.). Readiness and Emergency Management for Schools Technical Assistance Center. https://rems.ed.gov/K12FERPA.aspx

[6]. 11.0 FERPA and HIPAA: What Threat Assessment Teams Need to Know. (n.d.). In Behavioral Threat Assessment and Management for Educators and Administrators. Texas School Safety Center. https://txssc.txstate.edu/tools/tam-toolkit/ferpa-hipaa

[7]. Does HIPAA Apply to Schools? (2020, January 9). HIPAA Journal. https://www.hipaajournal.com/does-hipaa-apply-to-schools/

[8]. Joint Guidance on the Application of FERPA and HIPAA to Student Health Records | Protecting Student Privacy. (n.d.). Retrieved January 27, 2022, from https://studentprivacy.ed.gov/resources/joint-guidance-application-ferpa-and-hipaa-student-health-records

[9]. FERPA and Virtual Learning during COVID-19 | Protecting Student Privacy. (n.d.). Retrieved January 27, 2022, from https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning-during-covid-19

[10]. FERPA and Virtual Learning Related Resources March 2020. (n.d.). 1.

[11]. Reeves, M., & McCarthy, C. (2021). Upholding Student Civil Rights and Preventing Disproportionality in Behavioral Threat Assessment and Management (BTAM). National Association of School Psychologists. http://www.nasponline.org/btam-sped

[12]. Family Educational Rights and Privacy Act (FERPA), 34 C.F.R. § 300.530 (1974).

[13]. Protecting Students with Disabilities. (2020). U.S. Department of Education Office for Civil Rights. https://www2.ed.gov/about/offices/list/ocr/504faq.html

[14]. Protecting Student Privacy While Using Online Educational Services. (n.d.). 14.

[15]. The Family Educational Rights and Privacy Act: Guidance for Reasonable Methods and Written Agreements. (2015). 9.

[16]. Richman Smith, J. (2019, September 23). Reporting Apps, Email Scanning, and Beyond: What Boards of Education Should Know About the Latest Trends in School Safety. School Law. https://www.ctschoollaw.com/2019/09/reporting-apps-email-scanning-and-beyond-what-boards-of-education-should-know-about-the-latest-trends-in-school-safety/