CALIFORNIA Child Abduction TASK FORCE

Child Abduction T.I.P.S.

(Training, Information, Practices & Strategy)

Vol. 14 December 1, 2020

New FERPA Guidance from the U.S. Department of

Education Relating to School Safety

By: Theresa Mullineaux on March 13, 2019

In February 2019, the U.S. Department of Education released new Family Educational Rights and Privacy Act ("FERPA") guidance about schools' and school districts' responsibilities under FERPA relating to disclosures of student information to school resource officers, law enforcement units, and other stakeholders to explain and clarify how FERPA protects student privacy while ensuring the health and safety of all in the school community. See: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs_2-5-19_0.pdf

FERPA permits schools and districts to disclose education records (and the personally identifiable information ("PII") contained in those records) without consent if the "school officials" have "legitimate educational interests" in the education records. Each school or school district must include in its annual notification what constitutes a "school official" and what constitutes a "legitimate educational interest." Law enforcement who are employees of a school or district, would typically be considered a "school official." Law enforcement that are off-duty police officers or school resource officers would typically be considered a "school official" if they fall into four specific categories. The categories include performing an institutional service or function for which the school or district would otherwise use employees, are under the "direct control" of the school or district with respect to the use and maintenance of the education records, are subject to FERPA's use and re-disclosure requirements in 34 CFR § 99.33(a) allowing PII from education records to be used only for the purposes for which the disclosure was made (e.g., to promote school safety and the physical security of students) and limits the re-disclosure of PII from education records, and meets the criteria specified in the school or district's annual notification of FERPA rights for being school officials with legitimate educational interests in the education records.

Additionally, FERPA health and safety emergency provision allows for a student's education records (and the PII contained in the records) to Public disclosed, without appropriate consent, to appropriate parties in order to address a specific and articulable threat of a health or safety emergency. An appropriate party is defined under FERPA as a party whose knowledge of such information is necessary to protect the health or safety of students or other persons. The emergency must be significant and articulable, like an impending natural disaster, a terrorist attack, a campus threat, or the outbreak of an epidemic disease. The exception is limited to the period of the emergency and does not allow for a blanket release of PII from a student's education records.

Under FERPA, "law enforcement unit" means any individual, office, department, division, or other component of a school or district, like police officers or security guards, that are authorized or designated by the school or district to (1) enforce any local, State, or federal law, or refer to appropriate authorities a matter for enforcement of any local, State, or federal law, against any individual or organization other than the agency or institution itself; or (2) maintain the physical security and safety of the agency or institution. There are several categories of records that an educational agency or institution may maintain that are not "education records" under FERPA, including records of a "law enforcement unit." These law enforcement unit records are records that are (1) created by a law enforcement unit; (2) created for a law enforcement purpose; and (3) maintained by the law enforcement unit. Because of this, these records may be disclosed without the parent or eligible student's consent to outside parties under FERPA.

What This Means for School Districts: The landscape of federal and state laws is ever evolving, especially in regards to school safety. School districts are advised to keep law enforcement unit records separately from education records. Additionally, having law enforcement unit officials who are "school officials" with "legitimate educational interests" will allow a school to disclose PII from a student's educational record, without appropriate consent, to its law enforcement unit officials so that they may perform their professional duties and assist with school safety matters.

Mullineaux, T. March 13, 2019. New FERPA Guidance from the U.S. Department Education Relating to School Safety. St. Louis, MO.

https://www.k-12legalinsights.com/2019/03/new-ferpa-guidance-from-the-u-s-department-of-education-relating-to-school-safety/

The Vigilant Parent in the ever-evolving digital age.

By: Lt. Steve Lagorio & Lt. Brian Spears

San Jose Police Department

With technology rapidly becoming more integrated in our society, parents need to be safe and keep your children safe from online predators. With the changes that COVID-19 has brought us, the frequency of video chat, access to computers and other technology-related communication devices in the United States has increased at an immeasurable rate. Computers are available to children in our homes, schools, public libraries, community youth centers, and countless other public places youth congregate. Smart phone devices with internet connectivity are becoming more and more common amongst youth. A smart phone can send or receive multimedia messages, which includes picture and video messaging. Smart phones are also capable of accessing various social media applications (Apps). These types of Apps enable the user to create, participate, and share information.

Unfortunately, evolving technology has also increased online victimization. Over the last several years, the aggressive marketing of sexual material on the internet has increased. Today's youth are receiving unwanted exposure to sexual solicitation material through pop-up ads and malicious software by simply using social media apps and/or gaming systems.

Child sexual offenders are utilizing technology to further victimize our youth. They are capitalizing on the anonymity the Internet offers to make direct contact with our unsuspected youth. These constant contacts segue into what a child might view as a trustworthy relationship and can lead to in-person meetings. These direct contacts expose our children to potential abductions. Below are some safety guidelines to help protect your family from online threats:

Internet Safety Guide for Parents

- Talk to your children about the dangers about being online and let them know that they can come to you if something or someone online makes them uncomfortable, even if they have made a mistake.
- Never give out personal information, nor should you allow your child to give out personal information, such as: addresses, phone numbers, names, or the name and location of your child's school. Do not include personal information in an online profile. Pedophiles often use profiles as a means for finding victims online.
- Keep the computer in a common area of the home, such as the family room. Computers with Internet access should not be kept in your child's room, nor should they be used when you are away from home. Periodically review your child's e-mail account.
- Become computer literate. Get to know the online websites your kids visit and the online services they use. Find out what type of information the sites offer, and whether there are website settings to restrict objectionable material. Learn chat room lingo.
- Many Internet service providers (ISPs) have tools, known as "filters," to help parents restrict the types of websites kids can access. Find out if your ISP offers filters and learn how to use them. There are also commercially available software programs designed to help parents monitor their children's computer activities.
- Do not allow your child to respond to messages or bulletin board items that are sexually suggestive, obscene, or threatening. Forward a copy of such messages to your ISP.
- Never allow your child to arrange an in-person meeting with someone they met online without your permission. In-person meetings should occur in a public place and you should accompany your child.

For more information please visit: https://www.svicac.org/

COMMITTEE MEMBERS:

- Megan Eschleman, Chair, California Clearinghouse Manager, Department of Justice, Missing & Unidentified Persons Section
- Erin Runnion, Vice-Chair, Founder, The Joyful Child Foundation
- Bridget Billeter, Deputy Attorney General, California Department of Justice, Office of the Attorney General
- Heidi Brennan, Deputy District Attorney, Sacramento County
- Joseph Brine II, Special Agent, FBI Squad C-1, Violent Crimes , Major Offenders
- Deanne Castorena, Deputy-in Charge, Los Angeles Co. District Attorney's Office-Child Abduction Section
- Xiomara Flores-Holguin, Specialized Response Bureau (MART, CSEC, ROU and LE Liaison), Los Angeles County Department of Children & Family Services
- Marlene Glusing, Legal Assistant, Merced Co. District Attorney's Office
- Stephen Lagorio, Lieutenant, San Jose Police Department
- Leslie A. Olson, MA, Program Manager, Sacramento Co. Department of Child Protective Services
- Ken Roberts, California Highway Patrol
- Brian Sullivan, Special Agent, Federal Bureau of Investigation
- Cari Teran, Marriage & Family Therapist, Private Practice
- Jannell Violi, Program Specialist, Orange Co. Department of Education