Privacy Technical Assistance Center
Student Privacy Policy Office
U.S. Department of Education
855.249.3072 privacyTA@ed.gov https://studentprivacy.ed.gov

A Parent's Guide for Understanding K-12 School Data Breaches

Computers and the internet are integral to our lives, from online shopping to paying our taxes. Schools use computer systems to provide better learning environments for students, reduce administrative overhead, and give parents more visibility into their children's education. However, schools, like every other organization, face continued challenges protecting the data in their systems from breaches.

This document aims to provide parents of K-12 students information to help understand what it means when your school has a data breach, as well as provide tools and best practices to help navigate the sometimes confusing process of protecting your children's data in the event of a breach.

What is a Data Breach?

Data breaches come in many different forms, from cyber criminals breaking into school data systems and stealing sensitive data about students or employees, to accidental disclosures due to errors or misconfigurations. For the purposes of this document, a data breach can be understood as any circumstance where a school's student data system is improperly accessed, compromised, or disclosed to a third party.

What about FERPA?

The Family Educational Rights and Privacy Act, commonly referred to as FERPA, is a federal law that, among other things, protects the privacy of personally identifiable information (PII) from education records. While FERPA does not explicitly address "data breaches," it generally prohibits the disclosure of PII from education records without prior written consent from the parent or eligible student (34 CFR § 99.30), unless one of FERPA's exceptions to the written consent requirement applies. FERPA does not require a school to notify a parent that information from their child's education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. Although not required under FERPA, a school may notify parents following a risk assessment or as required by applicable state law.

State laws usually refer to data breaches by attributes such as the type or volume of data involved. More information on your state's data breach laws can be found through your state's Office of Attorney General or through certain nonprofit organizations.

There Was a Data Breach; What Now?

So, you have been notified, or otherwise became aware, that your or your child's information has been involved in a data breach at your school. It can be alarming to hear this news, but there are some immediate steps that you can take to better understand what happened and reduce the risk of any negative consequences:

1. Get confirmation that your or your child's data were affected.

   Many times, parents hear about a breach through media reports or by word of mouth. Reach out to your school and ask them to validate that your child's information was involved in the breach. Keep in mind that in the early stages of a data breach investigation, the extent of the breach may not yet be fully known.

2. Determine the risk to you or your child

   If your or your child's information is involved in the breach, one of the first things you should do is evaluate what kinds of data were involved to determine the risk that the loss or exposure of these data poses. Disclosure of some data, such as social security numbers, date of birth, account numbers, passwords, or other sensitive data can lead to fraud, identity theft, and similar crimes. Disclosure of other information such as grades, pictures, names, or addresses, while still personally identifiable, may not carry the same risk of negative outcomes.

3. Take steps to reduce the risk of negative impacts

   Once you understand what data were involved, you should think about ways to reduce the risk that the data may be used for harmful purposes. The following steps will depend on the types and sensitivities of the data that were exposed because of the breach:

   - Check your school's website often, and be alert for letters from the school to get updates on the breach.
   - Think about changing account passwords, ensuring that they are complex and unique.
   - Check your credit report for unauthorized activity or notify credit bureaus or the Internal Revenue Service (IRS).
   - Report to state or local law enforcement if there is indication of identify theft or other criminal activity.
   - Obtain some form of credit or identity theft monitoring (this often is offered by the school in cases where sensitive information was involved).
   - Monitor your financial, email, and social media accounts for unexpected activity.

4. File a Complaint

   If your child's information is involved in a data breach, it is always best to reach out to your school or district and verify the facts. If they are unable to address your concerns appropriately and you believe your rights under FERPA have been violated, you may file a complaint with the Student Privacy Policy Office (SPPO) by visiting https://studentprivacy.ed.gov/file-a-complaint. Complaints must

   - be filed by the parent or eligible student with FERPA rights regarding the education records that are the subject of the complaint;
   - be filed within 180 days of the alleged violation or within 180 days after you knew or reasonably should have known about the violation; and
   - contain specific allegations of fact giving reasonable cause to believe that a FERPA violation has occurred.

How the U.S. Department of Education Can Help

The U.S. Department of Education has a variety of resources to assist you when information from your child's education records is involved in a data breach. The Department's Student Privacy Policy Office (SPPO) and its Privacy Technical Assistance Center (PTAC) are available to answer your student privacy questions. We have resources and guidance available on our website, ranging from online videos for parents explaining your rights under FERPA to our extensive library of documents explaining best practices in student privacy and data security. We also have resources to help you understand your options for filing a complaint if you believe that your rights under FERPA have been violated.

You can reach us anytime through our website at https://studentprivacy.ed.gov, via email at PrivacyTA@ed.gov, or by phone at 855-249-3072.

Additional Resources

- What Parents Need to Know About Their Student's Data — https://studentprivacy.ed.gov/training/what-parents-need-know-about-their-students-data
- U.S. Department of Education Student Privacy Policy Office (SPPO) FERPA Complaint Information — https://studentprivacy.ed.gov/file-a-complaint
- Federal Trade Commission (FTC) Identity Theft Reporting & Recovery Tool — https://www.identitytheft.gov/
- Warning Signs of Identity Theft — https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
- Taxpayer Guide to Identity Theft — https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft