

08/26/2013

By Administrator

Schools collect a lot of personal information about students – information that, in the wrong hands, could be used for identity theft. Children and young adults are tempting targets for identity thieves because they usually have unblemished credit histories and no criminal records. Fraudsters can use their Social Security numbers and other personal information to open credit accounts, apply for jobs, rent apartments, obtain medical services and, even scarier, to impersonate them if they get into trouble with the law.

Under the [Family Educational Rights and Privacy Act](#), a federal law that applies to schools which receive funds from the U.S. Department of Education, parents have certain rights concerning their children's school records (these rights transfer to what is called the "eligible student" once the child reaches age 18 or attends school beyond high school).

To protect the privacy of information in school records, the law requires written permission from the parents or eligible students before it can be released. There are some exceptions. One big loophole is that schools don't need consent to disclose "directory" information such as a student's name, address, telephone number, and date and place of birth. But parents and eligible students must be notified if this information is going to be released and given enough time to say "no" if they wish. They also have the right to see the records and correct any errors.

Another law, the [Protection of Pupil Rights Amendment](#), requires parents' written consent before students under age 18 can be made to participate in any survey or study funded by the U.S. Department of Education that collects sensitive information, such as sex behavior and attitudes.

Parents should also be aware that some programs that take place at school but aren't officially school-sponsored may collect children's personal information, and those records are not covered by federal law. So it's important for parents to check the sponsors' privacy policies to understand what information is collected, how it is used, and what control, if any, they may

have. The Federal Trade Commission provides good [advice](#) for parents about the steps they should take to protect their children's identities from misuse and what to do if children become identity theft victims.

Some final recommendations for back-to-school privacy safety: Even if a school is not subject to federal laws because it does not receive federal funds, how it handles its records may be covered by state laws. Check with the state or local consumer protection agency where the school is located. And parents and students should let schools know if they have any concerns about the privacy or security of personal information. For example, using students' Social Security numbers as their school ID numbers needlessly exposes that information to possible identity theft and abuse. If a school does so, insist that it change this practice or at least offer the option to use random numbers instead.