Five Principles to Protect Student Privacy

The Parent Coalition for Student Privacy believes that the following five principles should be incorporated into any law or policy regarding the protection of personal student data in grades preK-12. After students reach age 18, all these rights, including those related to notification and consent, should devolve to them:

1. *Transparency*: Parents must be notified by their children's school or district in advance of any disclosure of personal student information to any persons, companies, or organizations outside of the school or district.

   All disclosures to third parties should also require publicly available contracts and privacy policies that specify what types of data are to be disclosed for what purposes, and provide a date certain when the data will be destroyed.

2. *No commercial uses*: Selling of personal student data and/or its use for marketing purposes should be banned. ***NO advertising should be allowed on instructional software or websites*** assigned to students by their schools, since ads are a distraction from learning and serve no legitimate educational purpose.

   While some of the current bills ban "targeted" ads, others ban targeted ads except for those derived from a student's one-time internet use. But how can any parent know whether an ad displayed to their child was based on data-mining their child a single time or over a longer period?

3. *Security protections*: At a minimum, there must be encryption of personal data at motion and at rest, and required training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor. Passwords should be protected in the same manner as all other personal student information.

   There must be notification to parents of all breaches, and indemnification of the same.

   No "anonymized" or "de-identified" student information should be disclosed without verifiable safeguards to ensure data cannot be easily re-identified.

4. *Parental/student rights*: NO re-disclosures by vendors or any other third parties to additional individuals, sub-contractors, or organizations should be allowed without parental notification and consent (or student, if they are 18 or older).

   Parents must be allowed to see any data collected directly from their child by a school or a vendor given access through the school, delete the data if it is in error or is nonessential to the child's transcript, and opt out of further collection, unless that data is part of their child's educational records at school.

   Any data mining for the purpose of creating student profiles, even for educational purposes, must be done with full parental knowledge.

Parental consent must be required for disclosure of personal data, especially for highly sensitive information such as their child's disabilities, health, and disciplinary information.

5. *Enforcement*: The law should specify fines if the school, district, or third party violates the law, their contracts, and/or privacy policies; with parents able to sue on behalf of their children's rights as well.

Without strong enforcement provisions, any law or policy protecting student privacy is likely to be ignored.