Model State Law
Chief Privacy Officer for Education Act
Version 2.0

Section 1. Title.

This Act shall be known and cited as the "Chief Privacy Officer for Education Act." This Act shall be liberally and remedially construed to effectuate its purpose. The purpose of the Act is to protect the privacy and security of personal information maintained by schools by creating the Office of the Chief Privacy Officer for Education to oversee, audit, consult, and report on matters that affect privacy and security of school records that contain personally identifiable information.

Section 2. Findings.

The Legislature finds:

(a) Privacy is a personal and fundamental right protected by Federal and State constitutional provisions and statutes.

(b) Records maintained by schools about students and others contain a wide range of personally identifiable information, often including health and financial information as well as information about educational activities. The use and disclosure of the information affects the rights and interests of those individuals and their families. In particular, information that schools maintain can permanently affect a student's educational, employment, and other future opportunities. Information that schools maintain about teachers, employees, alumni, contributors, school board members, and others can affect the future of those individuals.

(c) Personally identifiable information maintained by schools is at risk of improper use and sharing through poor privacy policies and practices; inadequate security; insufficient rules and guidance; and lack of training.

(d) Parents, students, and others are increasingly expressing concern and frustration about privacy, security, and sharing of personally identifiable information by schools.

(e) Cloud computing and other types of data storage and sharing under the control of third parties, especially those in other jurisdictions, can exacerbate existing risks as well as raise new risks. Among these risks are that cloud computing providers may claim ownership rights over personally identifiable information that schools store in the cloud; that third parties will use or disclose personally identifiable information about students improperly or without the knowledge or consent of schools, students, and parents; that personally identifiable data is at greater risk for security breaches, and that data storage and sharing with inadequate attention to the allocation of rights and responsibilities of all parties will harm students, parents, and others, and will raise costs and legal risks of schools.

(f) Lack of adequate privacy and security controls and a lack of understanding of the rights of students and parents, especially over student directory information, result in more personally identifiable information about students becoming public, increase the risk that students will become victims of identity theft, threaten the physical safety of some students, and allow for unregulated commercial use of student information.

(g) Schools and others that maintain personally identifiable information about students and others would greatly benefit from an authoritative source of privacy and security assistance focused on the risks that can affect the records they maintain. Students, parents, and others would also benefit.

Section 3. Definitions

(a) "Covered organization" means a school, a State agency that processes personally identifiable information for or from schools, and a contractor, grantee, or researcher that processes personally identifiable information for or from schools.

(b) "Personally identifiable information" means information about an individual processed by a covered organization, including any of the following:

(1) first and last name;

(2) home or other physical address, including street name and city or town;

(3) e-mail address;

(4) telephone number;

(5) social security number or other code or account number assigned to an individual, including a student identification number;

(6) IP address;

(7) fingerprint or photograph;

(8) any other identifier that permits the physical or online contacting of a specific individual;

(9) any representation of information that permits the identity of the individual to whom the information applies to be reasonably inferred by either direct or indirect means.

(c) "Processing" means with respect to personally identifiable information the collection, use, disclosure, maintenance, storage, erasure, or destruction of the personally identifiable information.

(d) "School" means any [public school, any non-public school of secondary education, any private school, any charter school, any for-profit school, and any school of higher education].

(e) "Security" means administrative, physical, and technical safeguards for personal information or information systems containing personal information.

Section 4. Appointment and Qualifications.

(a) There is hereby created in the State [Department of Education] the Office of Chief Privacy Officer for Education.

(b) The Governor shall appoint the Chief Privacy Officer for Education, who must be qualified by training or experience in privacy, civil liberties, information technology, or information security, and who shall take office upon confirmation by a majority of the membership of the Senate and a majority of the membership of the Assembly.

(c) The Chief Privacy Officer for Education shall serve for a term of five years and may be reappointed to one additional term of five years.

(d) The Chief Privacy Officer for Education may continue to serve in office after the expiration of his or her term of office until a successor is appointed and confirmed.

(e) The Chief Privacy Officer for Education may not be removed from office except for neglect of duty or malfeasance in office.

(f) The Chief Privacy Officer for Education shall receive salary and benefits equivalent to [xxx].

Section 5. Functions

(a) The functions of the Chief Privacy Officer for Education include but are not limited to:

(1) promoting the implementation of fair information practices for privacy and security of personally identifiable information processed by covered organizations;

(2) providing direct or indirect assistance or advice on privacy and security matters to covered organizations, students, parents, school organizations, State agencies, the legislature, and others as the Chief Privacy Officer for Education deems appropriate;

(3) advising students, parents, and other individuals about options and actions that they can take to protect the privacy and security of personally identifiable information;

(4) making recommendations on privacy and security to the Legislature, Governor, Department of Education, Federal Department of Education, covered organizations, students, parents, and school organizations;

(5) conducting oversight or audits of privacy and security activities at covered organizations;

(6) preparing privacy impact assessments for activities affecting privacy or security at covered organizations, and commenting on privacy impact assessments prepared by others;

(7) publishing model privacy and security policies and best practices for covered organizations, including standards for –

(A) privacy impact assessments;
(B) minimizing the processing of personally identifiable information, including the retention of the information;
(C) anonymizing personally identifiable information;
(D) the maintenance of audit logs that record information on the use or disclosure of personally identifiable information;
(E) responding to security breaches and providing notification to affected individuals;
(F) the use and disclosure of directory information about students, including standards for schools that allow students and parents to opt-out of disclosures of directory information;
(G) privacy and security obligation that should apply when covered organizations outscource the processing of personally identifiable information;
(H) disclosure of information about student athletes, student award recipients, and other student accomplishments;
(I) access by officials of covered organizations to social networking sites maintained by students, parents, and other individuals;
(J) the use of cloud computing services;
(K) public notices that describe the processing of personally identifiable information by covered organizations;
(L) Sharing of personally identifiable information with other states, nonprofit organizations, education technology companies, content providers and developers; and
(M) use of personally identifiable information for research and statistical purposes by covered organizations and by others.

(8) cooperating with other States and with the Federal government on privacy and security matters;

(9) promoting or conducting voluntary and mutually agreed upon nonbinding arbitration and mediation of privacy-related or security-related disputes involving schools where appropriate;

(10) receiving complaints from parents, students, and other individuals concerning the processing of personally identifiable information by covered organizations and, within the limits of available resources, providing advice, information, and referrals in response to the complaints;

(11) providing or sponsoring training in privacy and security for covered organizations and others affected by this Act;

(12) preparing and distributing lesson plans and other materials that will allow teachers to teach students about privacy and privacy rights;

(13) maintaining a public web page providing information and resources about privacy and security; and

(14) proposing legislation or commenting upon legislation pending before the Legislature that affects any activity within the scope of this Act.

(b) The Chief Privacy Officer for Education shall report directly to the [Commissioner of Education] and may report directly to the Governor and to the Legislature when the Chief Privacy Officer for Education deems it appropriate.

(c) The Chief Privacy Officer for Education shall submit an annual report directly to the [Legislature], Governor, [Commissioner of Education], and public, and may submit additional reports as the Chief Privacy Officer sees fit. The annual report shall include a summary of activities, recommendations, publications, and complaints received about privacy violations, and other matters.

Section 6. Powers

The Chief Privacy Officer for Education shall have the following powers:

(a) to access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by covered organizations that relate to privacy and security matters relevant to activities authorized under this Act;

(b) for any privacy or security matter relevant to activities authorized under this Act, to (1) conduct public hearings; (2) require by subpoena the production of records, reports, audits, reviews, documents, papers, recommendations, and other materials, and (3) compel the attendance of witnesses;

(c) to enforce a subpoena in any court of competent jurisdiction using counsel (1) hired by or otherwise available to the Chief Privacy Officer for Education; or (2) provided by the Attorney General or the [Secretary of Education].

(d) to administer to or take from any person an oath, affirmation, or affidavit, whenever appropriate in the performance of responsibilities under this Act;

(e) to review and comment upon any [State Department of Education] program, proposal, grant, or contract that involves the processing of personally identifiable information before the [Secretary of Education] begins or awards the program, proposal, grant, or contract;

(f) to hire employees and enter into contracts.

Section 7. Effective Date

This Act shall take effect 60 days after the date of enactment.