

General Personnel

Responsibilities Concerning Internal Information ¹

District employees are responsible for maintaining: (1) the integrity and security of all internal information, and (2) the privacy of confidential records, including but not limited to: student school records, personnel records, and the minutes of, and material disclosed in, a closed School Board meeting. Internal information is any information, oral or recorded in electronic or paper format, maintained by the District or used by the District or its employees. The Superintendent or designee shall manage procedures for safeguarding the integrity, security, and, as appropriate, confidentiality of internal information.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

¹ State and federal law controls the content of this policy to the extent that: (1) the unauthorized disclosure of student school records is prohibited by the Family Educational Rights and Privacy Act, (20 U.S.C. § 1232g); and the Illinois School Student Records Act, (105 ILCS 10/); (2) ~~the Freedom of Information Act (FOIA) (5 ILCS 140/7) exempts from disclosure certain private or personal information, employee evaluations, protects school security and response plans, and maps from disclosure;~~ (3) if a district offers a self-insured group health plan or flexible spending account, it must establish clear procedures to protect the employees' health information (45 C.F.R. §164.502); (4) ~~the Freedom of Information Act contains exemptions for certain private or personal information and employee evaluations (5 ILCS 140/7);~~ (5) the Ill. Personnel Record Review Act governs the release of an employee's disciplinary action (820 ILCS 40-); and (6) any person who knowingly destroys, removes, conceals, or alters any public record with the intent to defraud any party commits a Class 4 felony (50 ILCS 205/4, ~~amended by P.A. 98-1063~~). These are examples of the laws requiring the safekeeping of district and school records.

This policy contains an item on which collective bargaining may be required. Any policy that impacts upon wages, hours, and terms and conditions of employment, is subject to collective bargaining upon request by the employee representative, even if the policy involves an inherent managerial right. If a local collective bargaining agreement contains a provision on these responsibilities, it will supersede this policy and the board policy should state, "Please refer to the applicable collective bargaining agreement following current Agreement: [actual title of Collective Bargaining Agreement (not including dates)]." For employees not covered, the policy should reflect the board's current practice.

This sample policy's intent is to safeguard district records accessed or created by employees. This includes protecting the district from unauthorized release of confidential records or the destruction of records. While the legal guidance is sparse, districts should take steps to avoid security breaches. Some districts may have more legal obligations than others. School districts that are considered "covered entities" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub.L. 104-191) are required to comply with the HIPAA Security/Privacy Rule. See ¶ 1 of policy 7:340, Student Records, for further discussion of HIPAA. Furthermore, districts that allow foreign exchange students to attend their schools may need to put safeguards in place in order to protect data that is transferred to the Student and Exchange Visitor Information System (SEVIS). See ¶ 18 of policy 7:50, School Admissions and Student Transfers To and From Non-District Schools, for further discussion of SEVIS.

To help maintain the integrity of records, districts should prevent their over-accumulation. Not all internal information must be preserved even if it is a *public record* for purposes of ~~FOIA the Freedom of Information Act, 5 ILCS 140/~~. According to the Local Records Act, (50 ILCS 205/), a record must be retained only when it contains: (1) evidence of the district's organization, function, policies, procedures, or activities; or (2) informational data appropriate for preservation. While this is a slippery slope without definitive parameters, recorded information may generally be deleted that are conversational or personal, meeting notices, spam, email of a transient nature, duplicate material sent from other staff members, and draft material. However, no district record, no matter its form, may be destroyed if it is subject to a litigation hold. See administrative procedure 2:250-AP2, Protocols for Record Preservation and Development of Retention Schedules. For guidance on Board member use and retention of email, see 2:140-E, *Guidance for Board Member Communications, Including Email Use.*

LEGAL REF.: Family Educational and Privacy Rights Act, 20 U.S.C. §1232g.
Uses and Disclosures of Protected Health Information; General Rules, 45 C.F.R.
§164.502.
Ill. Freedom of Information Act, 5 ILCS 140/
Local Records Act, 50 ILCS 205/
105 ILCS 10/
Personnel Record Review Act, 820 ILCS 40/.

CROSS REF.: 2:140 (Communications To and From the Board), 2:250 (Access to District
Public Records), 5:150 (Personnel Records), 7:340 (Student Records)

DRAFT