Operations

Administrative Procedure – Treatment of Personally Identifiable Information Under Grant Awards

This procedure implements identification, handling, storage, access, disposal, and the overall confidentiality of personally identifiable information under grant awards in the subhead **Treatment of Personally Identifiable Information Under Grant Awards** in Board policy 4:15, *Identity Protection*. Use it when the District is a recipient of a federal grant award or State grant award governed by the Grant Accountability and Transparency Act (GATA) (30 ILCS 708/) and, as a result, must handle personally identifiable information (defined below) in its administration of the award.

Definitions

Personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books and public Web sites. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII (or *protected personally identifiable information*) whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual. 2 C.F.R. §200.1.

Protected personally identifiable information (Protected PII) is a subset of PII; it means an individual's first name or first initial and last name in combination with any one or more types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal records, medical records, financial records, or educational transcripts. Protected PII does not include personally identifiable information that is required by law to be disclosed. 2 C.F.R. §200.1.

Safeguarding Requirement

GATA and 2 C.F.R. §200.303(e) require grant recipients to take reasonable measures to safeguard (1) *protected personally identifiable information*, (2) other information that the awarding or pass-through agency designates as sensitive, such as *personally identifiable information*, and (3) information that the District considers to be sensitive consistent with applicable laws regarding privacy and confidentiality (collectively referred to in this Procedure as *sensitive information*).

The Superintendent or designee will ensure that the District:

1. Implements reasonable security measures, such as physical and technological safeguards, for the protection of sensitive information that meets or exceeds industry standards designed to protect such information from unauthorized access, destruction, use, modification, or disclosure.
2. Complies with all applicable laws, such as the Identity Protection Act (5 ILCS 179/) (IPA), Personal Information Protection Act (815 ILCS 530/10) (PIPA) and Student Online Personal Protection Act (105 ILCS 85/27) (SOPPA) in the event of a breach of sensitive information.
3. Notifies, if appropriate, members of the school community impacted by a breach when notification is not specifically required by law.
4. Educates staff members involved in the administration of grants that in addition to federal regulation 2 C.F.R. §200.303(e) and the terms of a specific award, multiple laws may apply to personally identifiable information, depending upon the type of information/record including: IPA

(5 ILCS 179/), PIPA (815 ILCS 530/), Family Educational Rights and Privacy Act, (20 U.S.C. 1232g), Ill. School Student Records Act (105 ILCS 10/), SOPPA (105 ILCS 85/), Personnel Record Review Act (820 ILCS 40/), and Local Records Act (50 ILCS 205/3).

5. Consults with the Board Attorney as needed to ensure compliance.

Relevant Board Policies, Administrative Procedures, and Exhibit for Handling of *Sensitive Information*

The following Board policies and administrative procedures also address and govern the District's identification, handling, storage, access, disposal, and overall confidentiality of certain types of sensitive information:

1. 2:220, *School Board Meeting Procedure*, and 2:220-E8, Sc*hool Board Records Maintenance Requirements and FAQs*, address storage, access, and destruction of meeting minutes, including closed meeting minutes and verbatim recordings.
2. 2:250, *Access to District Public Records*, addresses providing access to public records in response to Freedom of Information Act requests and the preservation and destruction of public records under the Local Records Act. 2:250-AP2, *Protocols for Record Preservation and Development of Retention Schedules*, also addresses the preservation and destruction of public records under the Local Records Act.
3. 4:15, *Identity Protection*, specifically requires the District to safeguard sensitive information under grant awards.
4. 4:80-AP1, *Checklist for Internal Controls*, requires the District to protect assets, including technology and electronic systems from loss or misuse.
5. 5:120-AP2, *Employee Conduct Standards*, requires all District staff members to respect the confidentiality of student and personal records and other information covered by confidentiality agreements.
6. 5:130, *Responsibilities Concerning Internal Information*, requires all District employees to maintain the integrity and security of all internal information and the privacy of confidential records.
7. 5:150, *Personnel Records*, and 5:150-AP, *Personnel Records*, address the identification, storage, and access to personnel records.
8. 6:235, *Access to Electronic Networks*, requires all users of the District's electronic networks to maintain the confidentiality of student information.
9. 6:235-AP1, *Acceptable Use of the District's Electronic Network*s, requires all users of the District's electronic networks to take steps to safeguard their integrity and security.
10. 7:340, *Student Records*, along with 7:340-AP1, *School Student Records*, and 7:340-AP2, *Storage and Destruction of School Student Records*, address the District's legal obligations regarding the identification, confidentiality, safeguarding, access, and disposal of school student records.
11. 7:345, *Use of Educational Technologies; Student Data Privacy and Security*, addresses the District's legal obligations regarding the handling and safeguarding of *covered information* that is shared with *operators*.

Disposal of Sensitive Information

When disposal of sensitive information is authorized by law and/or Board policy, the Superintendent or other administrator overseeing the administration of the grant award will ensure the District follows the disposal standard under PIPA (815 ILCS 530/40) and renders the information unreadable, unusable, and undecipherable.

Training for Employees and Contractors

District employees and contractors responsible for the administration of a federal or State award for the District will receive training on the safeguarding of sensitive information.

The Superintendent or designee will ensure:

1. Employees receive training upon their assignment to perform work under the award and then on a bi-annual basis thereafter, until the award is concluded or an employee's involvement in the award is complete, whichever is earlier. The training shall include education on this procedure and the District's policies and procedures listed above that govern the District's handling of sensitive information for various types of information/records.
2. Documentation of employee training on the handing of personally identifiable information is maintained, including the dates(s) of the training and attendance/completion of the training.
3. District contractors performing work under the grant award regularly receive training from the District or other comparable training on the management of sensitive information.

Resources

Ill. State Board of Education –

Checklist for Protection of Personally Identifiable Information, at www.isbe.net/Pages/Federal-and-State-Monitoring.aspx.

U.S. Dept. of Education –

Privacy Technical Assistance Center's Protecting Student Privacy Service, at www.studentprivacy.ed.gov.

Ill. Attorney General –

www.illinoisattorneygeneral.gov/consumer-protection/identity-theft

APPROVED: