Operational Services

Identity Protection

The collection, storage, use, and disclosure of social security numbers by the School District shall be consistent with State and federal laws. The goals for managing the District's collection, storage, use, and disclosure of social security numbers are to:

1. Limit all activities involving social security numbers to those circumstances that are authorized by State or federal law.
2. Protect each social security number collected or maintained by the District from unauthorized disclosure.

The Superintendent is responsible for ensuring that the District complies with the Identity Protection Act, 5 ILCS 179/. Compliance measures shall include each of the following:

1. All employees having access to social security numbers in the course of performing their duties shall be trained to protect the confidentiality of social security numbers. Training should include instructions on the proper handling of information containing social security numbers from the time of collection through the destruction of the information.
2. Only employees who are required to use or handle information or documents that contain social security numbers shall have access to such information or documents.
3. Social security numbers requested from an individual shall be provided in a manner that makes the social security number easily redacted if the record is required to be released as part of a public records request.
4. When collecting a social security number or upon request by an individual, a statement of the purpose(s) for which the District is collecting and using the social security number shall be provided.
5. Notification to an individual whenever his or her personal information was acquired by an unauthorized person; *personal information* is an individual's name in combination with his or her social security number, driver's license number or State identification card number, or financial account information.
6. Disposal of materials containing personal information in a manner that renders the personal information unreadable, unusable, and undeciperable; *personal information* has the meaning stated in #5, above.
7. All employees must be advised of this policy's existence and a copy of the policy must be made available to each employee. The policy must also be made available to any member of the public, upon request.

No District employee shall collect, store, use, or disclose an individual's social security number unless specifically authorized by the Superintendent. This policy shall not be interpreted as a guarantee of the confidentiality of social security numbers and/or other personal information. The District will use best efforts to comply with this policy, but this policy should not be construed to convey any rights to protection of information not otherwise afforded by law.

LEGAL REF.: 5 ILCS 179/, Identity Protection Act.

CROSS REF: 2:250 (Access to District Public Records), 5:150 (Personnel Records), 7:340 (Student Records)

Adopted by Board Action April, 2011
Amended by Board Action September, 2015

General Personnel

Personal Technology and Social Media; Usage and Conduct

Definitions

Includes - Means "includes without limitation" or "includes, but is not limited to."

Social media - Media for social interaction, using highly accessible communication techniques through the use of web-based and mobile technologies to turn communication into interactive dialogue. This includes *Facebook*, *LinkedIn*, *MySpace*, *Twitter*, and *YouTube*.

Personal technology - Any device that is not owned or leased by the District or otherwise authorized for District use and: (1) transmits sounds, images, text, messages, videos, or electronic information, (2) electronically records, plays, or stores information, or (3) accesses the Internet, or private communication or information networks. This includes laptop computers (e.g., laptops, ultrabooks, and chromebooks), tablets (e.g., iPads®, Kindle®, Microsoft Surface®, and other Android® platform or Windows® devices), smartphones (e.g., iPhone®, BlackBerry®, Android® platform phones, and Windows Phone®), and other devices (e.g., iPod®).

Usage and Conduct

All District employees who use personal technology and social media shall:

1. Adhere to the high standards for appropriate school relationships required by policy 5:120, *Ethics and Conduct* at all times, regardless of the ever-changing social media and personal technology platforms available. This includes District employees posting images or private information about themselves or others in a manner readily accessible to students and other employees that is inappropriate as defined by policy 5:20, *Workplace Harassment Prohibited*; 5:120, *Ethics and Conduct*; 6:235, *Access to Electronic Networks*; 7:20, *Harassment of Students Prohibited*; and the Ill. Code of Educator Ethics, 23 Ill.Admin.Code §22.20.
2. Choose a District-provided or supported method whenever possible to communicate with students and their parents/guardians.
3. Not interfere with or disrupt the educational or working environment, or the delivery of education or educational support services.
4. Comply with policy 5:130, *Responsibilities Concerning Internal Information*. This means that personal technology and social media may not be used to share, publish, or transmit information about or images of students and/or District employees without proper approval. For District employees, proper approval may include implied consent under the circumstances.
5. Refrain from using the District's logos without permission and follow Board policy 5:170, *Copyright*, and all District copyright compliance procedures.
6. Use personal technology and social media for personal purposes only during non-work times or hours. Any duty-free use must occur during times and places that the use will not interfere with job duties or otherwise be disruptive to the school environment or its operation.
7. Assume all risks associated with the use of personal technology and social media at school or school-sponsored activities, including students' viewing of inappropriate Internet materials through the District employee's personal technology or social media. The Board expressly

disclaims any responsibility for imposing content filters, blocking lists, or monitoring of its employees' personal technology and social media.

8. Be subject to remedial and any other appropriate disciplinary action for violations of this policy ranging from prohibiting the employee from possessing or using any personal technology or social media at school to dismissal and/or indemnification of the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of this policy.

The Superintendent shall:

1. Inform District employees about this policy during the in-service on educator ethics, teacher-student conduct, and school employee-student conduct required by Board policy 5:120, *Ethics and Conduct*.
2. Direct Building Principals to annually:
   a. Provide their building staff with a copy of this policy.
   b. Inform their building staff about the importance of maintaining high standards in their school relationships.
   c. Remind their building staff that those who violate this policy will be subject to remedial and any other appropriate disciplinary action up to and including dismissal.
3. Build awareness of this policy with students, parents, and the community.
4. Ensure that no one for the District, or on its behalf, requests of an employee or applicant access in any manner to his or her social networking website or requests passwords to such sites.
5. Periodically review this policy and any procedures with District employee representatives and electronic network system administrator(s) and present proposed changes to the Board.

LEGAL REF.: 105 ILCS 5/21B-75 and 5/21B-80.
Ill. Human Rights Act, 775 ILCS 5/5A-102.
Code of Ethics for Ill. Educators, 23 Ill.Admin.Code §22.20.
Garcetti v. Ceballos, 547 U.S. 410 (2006).
Pickering v. High School Dist. 205, 391 U.S. 563 (1968).
Mayer v. Monroe County Community School Corp., 474 F.3d 477 (7th Cir. 2007).

CROSS REF.: 5:20 (Workplace Harassment Prohibited), 5:30 (Hiring Process and Criteria), 5:120 (Ethics and Conduct), 5:130 (Responsibilities Concerning Internal Information), 5:150 (Personnel Records), 5:170 (Copyright), 5:200 (Terms and Conditions of Employment and Dismissal), 6:235 (Access to Electronic Networks), 7:20 (Harassment of Students Prohibited), 7:340 (Student Records)

Adopted by Board Action March, 2012
Amended by Board Action September, 2015