

Employee Ethics; Conduct; and Conflict of Interest (Policy 5:120)

All District employees are expected to maintain high standards in their school relationships, to demonstrate integrity and honesty, to be considerate and cooperative, and to maintain professional and appropriate relationships with students, parents, staff members, and others. In addition, the *Code of Ethics for Illinois Educators*, adopted by the Illinois State Board of Education, is incorporated by reference into this policy. Any employee who sexually harasses a student, willfully or negligently fails to report an instance of suspected child abuse or neglect as required by the Abused and Neglected Child Reporting Act (325 ILCS 5/), engages in *grooming* as defined in 720 ILCS 5/11-25, engages in grooming behaviors, violates boundaries for appropriate school employee student conduct, or otherwise violates an employee conduct standard will be subject to discipline up to and including dismissal.

The Superintendent or designee shall identify appropriate employee conduct standards and provide them to all District employees. Standards related to school employee student conduct shall, at a minimum:

1. Incorporate the prohibitions noted in paragraph 1 of this policy;
2. Define prohibited grooming behaviors to include, at a minimum, *sexual misconduct*. *Sexual misconduct* is (i) any act, including but not limited to, any verbal, nonverbal, written, or electronic communication or physical activity, (ii) by an employee with direct contact with a student, (iii) that is directed toward or with a student to establish a romantic or sexual relationship with the student. Examples include, but are not limited to:
 1. A sexual or romantic invitation
 2. Dating, or soliciting a date
 3. Engaging in sexualized or romantic dialog
 4. Making sexually suggestive comments that are directed toward or with a student
 5. Self-disclosure or physical exposure of a sexual, romantic, or erotic nature
 6. A sexual, indecent, romantic, or erotic contact with the student
3. Identify expectations for employees to maintain professional relationships with students, including expectations for employee-student boundaries based upon students' ages, grade levels, and developmental levels. Such expectations shall establish guidelines for specific areas, including but not limited to:
 1. Transporting a student
 2. Taking or possessing a photo or video of a student
 3. Meeting with a student or contacting a student outside the employee's professional role
4. Reference employee reporting requirements of the Abused and Neglected Child Reporting Act (325 ILCS 5/), Title IX of the Education Amendments of 1972 (20 U.S.C. §1681 et seq.), and the Elementary and Secondary Education Act (20 U.S.C. § 7926);
5. Outline how employees can report prohibited behaviors and/or boundary violations pursuant to Board policies 2:260, *Uniform Grievance Procedure*; 2:265, *Title IX Sexual Harassment Grievance Procedure*; and 5:90, *Abused and Neglected Child Reporting*; and
6. Reference required employee training related to educator ethics, child abuse, grooming behaviors, and boundary violations as required by law and policies 2:265, *Title IX Sexual Harassment Grievance Procedure*; 4:165, *Awareness and Prevention of Child Sexual Abuse and Grooming Behaviors*; 5:90, *Abused and Neglected Child Reporting*; and 5:100, *Staff Development Program*.

Statement of Economic Interests

The following employees must file a *Statement of Economic Interests* as required by the Ill. Governmental Ethics Act:

1. Superintendent;
2. Building Principal;
3. Head of any department;
4. Any employee who, as the District's agent, is responsible for negotiating one or more contracts, including collective bargaining agreement(s), in the amount of \$1,000 or greater;
5. Hearing officer;
6. Any employee having supervisory authority for 20 or more employees; and
7. Any employee in a position that requires an administrative or a chief school business official endorsement.

Ethics and Gift Ban

School Board policy 2:105, *Ethics and Gift Ban*, applies to all District employees. Students shall not be used in any manner for promoting a political candidate or issue.

Prohibited Interests; Conflict of Interest; and Limitation of Authority

In accordance with Section 22-5 of the School Code, "no school officer or teacher shall be interested in the sale, proceeds, or profits of any book, apparatus, or furniture used or to be used in any school with which such officer or teacher may be connected," except when the employee is the author or developer of instructional materials listed with the Illinois State Board of Education and adopted for use by the Board. An employee having an interest in instructional materials must file an annual statement with the Board Secretary.

For the purpose of acquiring profit or personal gain, no employee shall act as an agent of the District nor shall an employee act as an agent of any business in any transaction with the District. This includes participation in the selection, award or administration of a contract supported by a federal award or State award governed by the Grant Accountability and Transparency Act (GATA) (30 ILCS 708/) when the employee has a real or apparent conflict of interest. A conflict of interest arises when an employee or any of the following individuals has a financial or other interest in the entity selected for the contract:

1. Any person that has a close personal relationship with an employee that may compromise or impair the employee's fairness and impartiality, including a member of the employee's immediate family or household;
2. An employee's business partner; or
3. An entity that employs or is about to employ the employee or one of the individuals listed in one or two above.

Employees shall neither solicit nor accept gratuities, favors, or anything of monetary value from contractors, potential contractors, or parties to agreements or contracts. Situations in which the interest is not substantial or the gift is an unsolicited item of nominal value must comply with State law and Board policy 2:105, *Ethics and Gift Ban*.

Outside Employment

Employees shall not engage in any other employment or in any private business during regular working hours or at such other times as are necessary to fulfill appropriate assigned duties.

Responsibilities Concerning Internal Information (Policy 5:130)

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.

Solicitations By or From Staff (Policy 5:140)

District employees shall not solicit donations or sales, nor shall they be solicited for donations or sales, on school grounds without prior approval from the Superintendent.

Identity Protection (Policy 4:15)

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. The stated reason for collection of the social security number must be relevant to the documented purpose.
5. If this policy is amended, employees will be advised of the existence of the amended policy and a copy of the amended policy will be made available to each employee.

The Superintendent is also responsible for ensuring the District complies with the Personal Information Protection Act, 815 ILCS 530/. Compliance measures shall include each of the following:

1. Written or electronic notification to an individual and, if applicable, the owner of the information or licensee, as required by 815 ILCS 530/10 whenever his or her personal information was acquired by an unauthorized person; *personal information* means either:
 1. An individual's first name or first initial and last name in combination with any one or more of his or her (i) social security number, (ii) driver's license number or State identification card number, (iii) financial account information (with any required

security codes or passwords), (iv) medical information, (v) health insurance information, and/or (vi) unique biometric data or other unique physical or digital representation of biometric data, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired through the breach of security; or

2. An individual's username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the username or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.
2. Cooperation with the owner of the information in matters relating to the breach, if applicable, as required by 815 ILCS 530/10.
3. Disposal of materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable; personal information has the meaning stated in #1, above.

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.

Internet Safety – Acceptable Use of District Computers and Use of District Means to Access the Internet (Policy 6:235)

Electronic networks are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication.

The term *electronic networks* includes all of the District's technology resources, including, but not limited to:

1. The District's local-area and wide-area networks, including wireless networks (WiFi), District-issued Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networks or to any District-issued online account from any computer or device, regardless of location;
3. District-owned or District-issued computers, laptops, tablets, phones, or similar devices.

The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate

online behavior, including but not limited to: (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyberbullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use. Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Users of the District's electronic networks have no expectation of privacy in any material that is stored on, transmitted, or received via the District's electronic networks. General rules for behavior and communications apply when using electronic networks. The District's administrative procedure, *Acceptable Use of the District's Electronic Networks*, contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials. Internet Safety

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the *Authorization for Access to the District's Electronic Networks* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use. Confidentiality

All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

Violations

The failure of any user to follow the terms of the District's administrative procedure, *Acceptable Use of the District's Electronic Networks*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

5:125 Personal Technology and Social Media: Usage and Conduct

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, but is not limited to, services such as *Facebook*, *LinkedIn*, *Twitter*, *Instagram*, *Snapchat*, 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/or social media shall:

1. Adhere to the high standards for **Professional and Appropriate Conduct** required by policy 5:120, *Employee Ethics; Conduct; and Conflict of Interest* 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*; 5:100, *Staff Development Program*; 5:120, *Employee Ethics; Conduct; and Conflict of Interest*; 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. Inform their immediate supervisor if a student initiates inappropriate contact with them via any form of personal technology or social media.
5. Report instances of suspected abuse or neglect discovered through the use of social media or personal technology pursuant to a school employee's obligations under policy 5:90, *Abused and Neglected Child Reporting Child Reporting*.
6. Not disclose student record information, including student work, photographs of students, names of students, or any other personally identifiable information about students, in compliance with policy 5:130, *Responsibilities Concerning Internal Information*. For District employees, proper approval may include implied consent under the circumstances.
7. Refrain from using the District's logos without permission and follow Board policy 5:170, *Copyright*, and all District copyright compliance procedures.
8. Use personal technology and social media for personal purposes only during nonwork 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.
9. 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.
10. 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, *Employee Ethics; Conduct; and Conflict of Interest*.
2. Direct School 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.
1. Build awareness of this policy with students, parents, and the community.
2. Ensure that neither the District, nor anyone on its behalf, commits an act prohibited by the Right to Privacy in the Workplace Act, 820 ILCS 55/10; i.e., the *Facebook Password Law*.
3. Periodically review this policy and any procedures with District employee representatives and electronic network system administrator(s) and present proposed changes to the Board.

School Board Policies

All employees are responsible for knowing and complying with the School Board policies and procedures. Policy reference books are available in Principals' offices and are also [available online](#). Should an employee have a question or wishes to review these policies they should confer with their building administration.