

## 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 smartphones such as BlackBerry®, Android®, iPhone®, and other devices, such as, iPads® and iPods®.

#### Usage and Conduct

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

1. Adhere to the high standards for appropriate school relationships in 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/Directors 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.

### **District Employees Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct**

1. The use of personal electronic device(s) on a school site is a privilege which the District grants to any District employee who is willing to assume the responsibility of abiding by the guidelines set forth in the Authorization for Electronic Network Access. District employees may only configure their personally owned devices with their district login credentials. Configuring student devices with District employee credentials is strictly prohibited. If District employees are found to be in violation of the District's Policy 6:235, *Access to Electronic Networks*, they may be directed to remove their personal electronic device(s) from the Quincy Public Schools Network. Any District employee who is suspected of violating the Access to Electronic Networks Policy or other District Policies will be referred to the District Administration and may be subject to disciplinary action.
2. District employees are responsible for physically securing their personal devices within their school site. The District assumes no responsibility or financial liability for any damage a District employee suffers, including but not limited to theft, physical damage, and loss of data or software malfunctions of the personal electronic device. If a personal electronic device appears to have been stolen, the District employee should immediately report the incident to his/her immediate superior.

3. District employees are strictly prohibited from using peer-to-peer file sharing software. The use of network monitoring software or applications considered invasive by the District is considered to be a serious offense, and will result in disciplinary actions.

#### Disclaimers

- A. Wireless access is available for the Internet only. Users of personal devices will not be granted access to other network resources such as school-system owned software and hardware devices including printers.
- B. The District's technology department personnel are not permitted to provide technical support for personal devices. Support and technical assistance is the sole responsibility of the user.
- C. The District reserves the right to disconnect personal devices or disable services without notification.
- D. The District reserves the right to discontinue the BYOT program at any time.

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 August 2013