Crafting a Comprehensive, Legally Sound Approach to Acceptable Technology Use

Presented By: Elena M. Gallegos & Karla A. Schultz

WALSH GALLEGOS
TREVIÑO KYLE & ROBINSON P.C.

1

Introduction

- Staff, students, and visitors are allowed to use district technology resources, such as computers, email and Wi-Fi.
- Districts also routinely issue district-owned technology devices like tablets to students, and cell phones, tablets, and laptops to staff.
- Has your district set out the rules for acceptable use of those resources?

2

What is an Acceptable Use Policy/Agreement?

- These are written guidelines that set out the terms for acceptable use of a district's technology resources, equipment, and services.
- Everyone using district technology resources should receive and sign such guidelines.

3

User Responsibilities and Expectations

- District policy, regulation, or agreement forms should explicitly say that:
  - Student and employee use of district technology resources should be used primarily for instructional and administrative purposes, consistent with the district's mission, goals, and objectives.
  - Use of district technology resources is a privilege, not a right.
  - Failure to properly use district technology will result in suspension or even termination of that privilege and may have other disciplinary consequences.

4

What Else?

- District policy, regulation, or acceptable use agreement forms should also include:
  - Definitions
  - Expectations for electronic behavior
  - Protocol for keeping devices and electronic information secure
  - Prohibited activities

5

NMSBA Model Policy IJNDB

- Policy IJNDB and related regulations are titled Use of Technology Resources in Instruction
  - Focus is only on instructional use. EIS = "electronic information services"
  - Policy incorporates requirement of the federal Children's Internet Protection Act
  - Requires "anyone who uses the EIS to receive instruction in and follow its guidelines and procedures for appropriate use."
  - "Instruction in appropriate online behavior shall include how to interact with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response."
  - "Anyone who misuses, abuses, or chooses not to follow the EIS guidelines and procedures will be denied access to the district's EIS and may be subject to disciplinary action."
  - "Each user will be required to sign an EIS user agreement." In some policies, IJNDB-E has a brief agreement.

6

NMSBA Model Policy EGD

- Policy EGD is titled Use of Technology in Office Services
  - It addresses:
    - "Electronic Communications" Records Retention
    - Compliance with the Open Meetings Act
    - Compliance with Inspection of Public Records Act
  - "Electronic communications (including records made with other software and sent in e-mail) which are sent or received by the Board or district employees pertaining to the business of the school may be subject to public disclosure and inspection as public records and discovery in litigation as evidence in support of a claim."

7

What About Limited Personal Use?

- Many districts issue technology devices to staff and students – laptops, cellular phones, email address and resources, etc.
- No doubt those devices are used not just for school purposes and business.
- Do your acceptable use policies, regulations, and/or procedures/forms permit some limited personal use of district's technology resources?
  - If not, your policies, regulations, and/or procedures should say what personal use is (and is not) allowed.
  - If so, be sure the policies, regulations, and/or procedures spell out the permissible parameters of such use.

8

Children's Internet Protection Act

- This law requires schools to:
  - Adopt and implement an Internet safety policy to restrict minors' access to obscene, pornographic, or harmful online content
  - Block or filter Internet access to such content
  - Monitor online activities of minors at school and on school devices
  - Educate students about appropriate online behavior
- Districts must comply with the federal Children's Internet Protection Act to receive certain discount rates.
- Usually, districts must annually certify compliance to the FCC.
- The requirements, and how the district meets them, should be explained in your policies, regulations, and/or procedures.

9

Monitoring Use of District Technology

- If it does not already say so, your acceptable use policy, regulations and/or agreements should expressly state that emails, texts, and other use of district technology resources by students, employees, or even members of the public, are not private, and that designated staff can monitor those district technology resources any time to be sure it is being appropriately used.
- To that end, your district will want to ensure that such designated staff are properly trained.

10

Search of Devices Assigned to Students

- 6.11.2.10 NMAC says: Search and seizure. School property assigned to a student and a student's person or property while under the authority of a public school are subject to search, and items found are subject to seizure, in accordance with the following requirements:

  (1) Notice of search policy. Students shall be given reasonable notice, through distribution of written policies or otherwise, of each school's policy on searches at the beginning of each school year or upon admission for students entering during the school year.

  (2) Who may search? Certified school personnel, school security personnel and school bus drivers are "authorized persons" to conduct searches when a search is permissible as set forth in Subsection B of 6.11.2.10 NMAC. An authorized person who is conducting a search may request the assistance of one or more people, who upon consent become authorized to search for the purpose of that search only.

  (3) When a search is permissible. Unless local school board policy provides otherwise, an authorized person may conduct a search when the authorized person has a reasonable suspicion that a crime or other breach of disciplinary rules is occurring or has occurred. An administrative authority may direct or conduct a search under the same conditions and also when the administrative authority has reasonable cause to believe that a search is necessary to help maintain school discipline.

11

Student Searches (continued)

(4) Conduct of searches and witnesses. The following requirements govern the conduct of permissible searches by authorized persons.

  (a) School property, including lockers and school buses, may be searched with or without students present unless a local school board or administrative authority provides otherwise. When students are not present for locker searches, another authorized person shall serve as a witness whenever possible. Locks furnished by students should not be destroyed unless a student refuses to open one or circumstances otherwise render such action necessary in the judgment of the administrative authority.

  (b) Student vehicles when on campus or otherwise under school control and students' personal effects, which are not within their immediate physical possession, may be searched in accordance with the requirements for locker searches in Subparagraph (a) of Paragraph (4) of Subsection B of 6.11.2.10 NMAC.

  (c) Physical searches of a student's person may be conducted only by an authorized person of the same sex as the student and, except when circumstances render it impossible, may be conducted only in the presence of another authorized person of the same sex. The extent of the search must be reasonably related to the infraction, and the search shall not be excessively intrusive in light of the student's age and sex, and the nature of the infraction.

12

Employee Searches

- While "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer," an employer's search of a pager assigned to an employee was reasonable and constitutional because it was "motivated by a legitimate work-related purpose, and because it was not excessive in scope." *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010).
- So even if there is a reasonable expectation of privacy in the employee's office area or work devices, a government employer's (i.e., school district's) search does not violate the Fourth Amendment when that search is for a non-investigatory, work-related purpose or an investigation of work-related misconduct.
- A school district does not need probable cause to search an employee's district issued property (e.g., computer, cell phone). The search is lawful if it is: (1) justifiable at its inception, and (2) reasonable in scope.

13

Security and Privacy Measures

- With the increasing digitization of school resources, safeguarding sensitive information and ensuring the privacy of users is essential.
- So, it is critical to protect against improper, and even unnecessary, access to information stored on the district's technology systems, including student and employee information.
- Therefore, the acceptable use policies, regulations, and/or procedures should set out mandatory security measures, including password protection, data encryption, and guidelines for handling confidential student or employee information.
- It should also address the importance of respecting confidentiality and reporting any potential security breaches promptly.

14

Digital Etiquette and Cyberbullying Prevention

- Acceptable use policies, regulations, and/or procedures should also set out clear expectations for respectful and lawful communication on district technology resources.
- This will include express prohibitions on accessing, uploading, downloading, storing, transmitting, receiving, or posting materials or images that are pornographic, obscene, sexually explicit, profane, vulgar, threatening, discriminatory, harassing, political, unlawful or disruptive to the educational process.
- Consider reiterating the state law prohibition on cyberbullying.
- Be sure your policies, regulations, and/or procedures tell users how to report violations of these protocol.

15

Prohibited Use of District Technology

- Acceptable use policies, regulations, and/or procedures should make clear what is unacceptable.
- Examples:
  - Accessing technology resources to alter, damage, or delete district property or information, or to otherwise breach electronic equipment or communications systems in violation of the law or district policies, regulations, and/or procedures.
  - Applying additional security walls, withholding passwords, or otherwise interfering with the district's ability to monitor use.
  - Disabling or attempting to disable or bypass any Internet filtering protocol.
  - Using someone's account without permission, or pretending to be someone else when posting, transmitting, or receiving messages.
  - Attempting to read, delete, copy, modify, or interfere with another person's use of technology resources.

16

Loss or Damage to District Technology

- What if an employee or student loses or damages district technology?
- How do you handle theft or wrongful access of district devices?
- Be clear that users may be held responsible for any loss or damage of district technology caused by intentional or negligent acts.
- Address consequences for failure to return the devices.

17

Off-Campus Use of District Technology Resources

- Typically staff and students are permitted some use of district technology resources at home and outside of school.
- Therefore, acceptable use policies, regulations, and/or procedures should make them aware that their off-campus use of those resources will be subject to the same acceptable use rules.
  - Include the obligation to keep devices, and information on them, secure.
- This means that even though they are off work or out of school, the use of district technology remains subject to monitoring and the prohibited uses.
- It is also important that users understand they do not own the information or files stored on the district technology.

18

Records Retention and Access

- District records includes electronic records.
- Be sure your acceptable use policies, regulations, and/or agreements ensure that employees understand their obligations about retention of electronic records regarding district business whether created or maintained using the district's technology resources or using personal technology resources.
- Also, ensure that you clearly notify employees that their use of district technology resources, including emails and text messages on those devices, are subject to the Inspection of Public Records Act.
- Retention of electronic records should be consistent with the district's records retention schedule.

19

Disclaimers

- Acceptable use policies, regulations, and/or procedures should note that use of district technology is at the user's own risk.
- Therefore, the district is not responsible for any damage a user may experience, such as loss, damage, or unavailability of data stored on district systems and devices.

20

Regular Review and Update

- Given the rapid changes in technology, acceptable use policies, regulations, and/or agreements should not be static.
- Regular reviews, ideally on an annual basis and with the assistance of IT staff, can ensure that your district policies, regulations, and/or procedures remain relevant and effective.

21

Elena M. Gallegos
Email: egallegos@wabsa.com

Karla Schultz
Email: kschultz@wabsa.com

500 Marquette Ave. N.W. Suite 1310
Albuquerque, NM 87106
Phone: 505-243-6864

22

The information in this presentation was prepared by Walsh Gallegos Treviño Kyle & Robinson P.C. It is intended to be used as general information only and is not to be considered specific legal advice. If specific legal advice is sought, consult an attorney.

23