UPDATE ON
PERSONAL TECHNOLOGY ISSUES IN SCHOOLS

Illinois Council of School Attorneys

November 21, 2014
Presented by:
John M. Izzo
Courtney N. Stillman
Sraga Hauser, LLC
www.sragahauser.com

I. What is "Personal Technology?"

II. Fourth Amendment Search and Seizure

A. Standard for searching student personal technology:

1. The *T.L.O.* standard applies when searching a student's personal technology – *i.e.*, the search must be (i) justified at its inception based on reasonable suspicion that the search will reveal evidence of the student's violation of law and/or school rules; and (ii) reasonable in scope based on objectives of the search and degree of intrusiveness under the circumstances.

2. When it comes to student cell phones, there must be a reasonable suspicion that a student's cell phone contains evidence of prohibited use or content before school personnel may review text messages, e-mails, pictures, etc. on the phone.

B. Conflicting Case Law on Student Technology Searches

1. ***Klump v. Nazareth Area School District***, 425 F.Supp. 2d 622 (E.D. Pa. 2006): High school had a policy permitting students to carry, but not use or display, cell phones during school hours. A student's cell phone fell out of his pocket and his teacher took it.

Teacher and assistant principal called all of the students listed in the phone to determine if they were violating the school's policy. The teacher and Assistant Principal searched the student's text messages and alleged that one of the messages referenced drug dealing. They also carried on a text message conversation with the student's brother without identifying themselves.

When the student to whom the cell phone belonged was disciplined, he sued the district. The court denied district defendants' motion to dismiss on the

basis of governmental immunity. Although the teacher was justified in seizing the phone under the school policy, there was no justification for searching the phone for evidence of other students' misconduct.

2. ***J.W. v. DeSoto County School District***, 2010 WL 4394059 (N.D. Miss. 2010):

   A student (J.W.) opened his cell phone in class to retrieve a text message from his father and the teacher confiscated the phone. School staff looked at the pictures on the phone and saw a picture of J.W. and another student with a BB gun.

   J.W. was expelled, based on the district's rule prohibiting students from displaying a gang symbol or any message associated with criminal activity at school.

   The student sued, but the court granted the district's motion to dismiss the case. Distinguishing this case from *Klump*, the *J.W.* court noted that in *Klump* the student's phone accidentally fell from his pocket. Here, however, the student knowingly used his cell phone at school and therefore had a diminished expectation of privacy in the phone.

3. ***G.C. v. Owensboro Public Schools***, 2013 WL 1235592 (6th Cir. 2013):

   Non-resident student began to have disciplinary problems as a freshman. He told school officials that he used drugs and had depression and anger issues. After a behavior incident in February, he told the Assistant Principal that he was very upset about an argument with his girlfriend and planned to kill himself.

   After another behavior incident in March, he told the Assistant Principal that he was still worried about the things he had discussed with her in February. Concerned about the student being suicidal, the Assistant Principal checked his cell phone to see if there was any indication that he was considering suicide.

   In September of his sophomore school year, *G.C.* was seen texting in class in violation of district policy. The teacher took his cell phone and brought it to another Assistant Principal, who then read four text messages "to see if there was an issue with which [she] could help him so that he would not do something harmful to himself or someone else."

   After this incident, the Superintendent decided to reverse the student's privilege of attending school in the district as a non-resident due to his texting in class. The student filed an action in federal court to maintain his enrollment in the district and seeking monetary damages for alleged violations of his 1st, 4th, and 5th Amendment rights.

The student argued (in part) that the September search of his cell phone was not supported by a reasonable suspicion that justified school officials reading his text messages. The district argued that the searches were limited and "aimed at uncovering any evidence of illegal activity" or indication that *G.C.* might hurt himself. After considering the rulings in the *J.W.* and *Klump* cases, the U.S. Court of Appeals for the 6th Circuit concluded that the "fact-based approach" taken in *Klump*, rather than the "blanket rule" set forth in *J.W.* should be applied in the *G.C.* case.

The court held that general background knowledge about drug abuse or depression, without more, does not enable school officials to search a student's cell phone when a search would otherwise not be justified. When school officials searched *G.C.*'s cell phone in September after he was seen sending two texts, they did not have any specific reason to believe that he was engaging in an unlawful activity or contemplating harming himself or others.

4. ***Gallimore v. Henrico County Sch. Bd.***, 2014 WL 3867557 (E.D. Va. 2014)

Administration received reports from two parents that a long haired student had smoked marijuana on a school bus that morning. Student was pulled out of class and administrators conducted a pat down search and searched backpack, pockets and shoes in privacy of office. They also searched the student's cell phone and other belongings.

The Court dismissed all of the student's claims other than the Fourth Amendment claim against the administrator who allegedly searched the phone. The Court held that taking all of Plaintiff's factual allegations as true, the pat down search was justified, but the search of the student's cell phone exceeded the scope of a reasonable search to find drugs. Unlike a sandwich bag or the student's Vaseline jar, his cell phone could not have contained drugs. Searching his cell phone was not "reasonably related" to the objective of the search, *i.e.*, finding evidence of drug use on bus earlier that day.

UPDATE: The parties reached an agreement and the complaint was withdrawn with prejudice.

C. Recent Supreme Court guidance: ***Riley v. California***, 134 S. Ct. 2473 (2014)

Supreme Court ruled that police officers who lawfully seized cell phones of criminal defendants upon arrest could search hardware for weapons and evidence of a crime to protect police and prevent the distribution of evidence. However, the Fourth Amendment prohibits searching digital contents of a cell phone, a "mini computer," without a warrant.

D. **Standard for public employee workplace search**:

A workplace search must be justified in its inception and reasonable in scope. It is justified in its inception if the employer has reasonable grounds to believe that the search will uncover evidence of the employee's misconduct. The search is reasonable in scope if measures taken by the employer are reasonably related to the search's objective and not overly intrusive in light of the nature of the alleged conduct. Reasonableness is measured on a case by case basis and depends upon balancing the public, governmental and private interests in a given situation. ***Gossmeyer v. McDonald*, 13 PERI 4020 (Ill. Ct. App. 1997).**

III. Privacy Rights

A. Privacy Settings for Social Media

1. ***R.S. v. Minnewaska Area Sch. Dist.***, 2012 WL 3870868 (D. Minn. 2012):

A parent complained to the school that *R.S.*, a sixth grader, was communicating with a boy via the internet about sexual topics. When questioned by school officials, *R.S.* admitted to the communication. She was called to the office of the school security officer and pressured into providing her Facebook password. *R.S.* felt humiliated as officials read not only the public messages on her wall, but also her private messages.

A reasonable expectation of privacy turns in large part on the person's ability to exclude others from the place searched. *R.S.* had a reasonable expectation of privacy in her personal electronic communications for which a password was required and which were not readily accessible to the general public.

Here there was no legitimate school interest of maintaining discipline in the classroom and on school grounds to balance against *R.S.'s* reasonable expectation of privacy because her messages occurred at home.

2. ***Roasio v. Clark County School Dist.***, 2013 WL 3679375 (D. Nev. 2013):

J.R. did not make the basketball team, but was placed on the team with certain conditions after his father protested. After the season's last game, *J.R.* tweeted obscene tweets about the coaches from a restaurant during dinner. One of his followers gave the tweets to school officials and *J.R.* was charged with cyberbullying.

When a person with a public privacy setting tweets, he intends that anyone can read the tweet, so there can be no reasonable expectation of privacy.

Court commented that a person with a private account has a better argument of expecting privacy, but still disseminates his postings to the public and may not be protected by the Fourth Amendment.

Even if *J.R.* had a private account, he took the risk that his follower would turn his tweet over to the government. A school may access Facebook and Twitter accessible only to "friends," through a friend without violating the Fourth Amendment.

3. ***Chaney v. Fayette County Pub. Sch. Dist.***, 977 F. Supp. 2d. 1308 (N.D. Ga. 2013)

   The district held a seminar on internet safety and social media. The technology director used in his presentation a picture of the student in a bikini standing next to a cut-out of Snoop Dogg as an example of how pictures posted to Facebook can be embarrassing. The student alleged it labeled her as promiscuous and an alcohol abuser.

   District policy prohibited employees from using electronic communication inappropriately and from disclosing information about students. Also, employees were required to notify a parent before interacting with a student by social media.

   Student had most inclusive privacy setting she could choose as a minor – a semi private setting allowing "friends" and "friends of friends" to view her Facebook page and pictures.

   To invoke the 4th Amendment, a person must show both a subjective expectation and the willingness of society to recognize the expectation as legitimate. The student did not have a legitimate expectation of privacy because she made her page available to hundreds and thousands of people she did not know (friends of friends). There is no legitimate expectation of privacy in information a person voluntarily turns over to third parties.

B. ***Privacy in the School Settings Act***, P.A. 098-0129 (eff. 1/1/14)

   An elementary or secondary school must provide notification to the student and his or her parent or guardian that the elementary or secondary school may request or require a student to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website if the elementary or secondary school has reasonable cause to believe that the student's account on a social networking website contains evidence that the student has violated a school disciplinary rule or policy. The notification must be published in the elementary or secondary school's disciplinary rules, policies, or handbook or communicated by similar means.

IV. First Amendment Issues

A. General Standards Regarding Student Speech in School

1. ***Tinker v. Des Moines Independent Sch. Dist.***, 393 U.S. 503 (1969) – expression causes or could reasonably lead school authorities to forecast a material and substantial disruption to the school's mission or instruction.

2. ***Bethel School Dist. No. 403 v. Fraser***, 478 U.S. 675 (1986) – lewd, vulgar, obscene or patently offensive expression.

3. ***Hazelwood v. Kuhlmeier***, 484 U.S. 260 (1988) – school sponsored publications.

4. ***Morse v. Frederich***, 551 U.S. 393 (2007) – expression that may be reasonably regarded as encouraging illegal use.

5. ***Lovell v. Poway Unified Sch. Dist.***, 90 F.3d 367 (9th Cir. 1996) – speech that constitutes a true threat of physical violence.

B. Sample Conflicting Case Law – Student Speech

1. ***Bradford v. Norwich City Sch. Dist.*, 2014 WL 4715638 (N.D. N.Y. 2014).**:

   Two students sent each other text messages off campus threatening to push student M.Y. down the stairs and assault her. The two students forwarded their text messages to E.K., a friend of M.Y. A teacher heard M.Y. reading the texts aloud to other students and saw that she was upset and crying. The two students asserted First and Fourteenth Amendments claims in district court.

   The court dismissed their First Amendment claim on the basis that under Tinker, it was reasonably foreseeable that the threatening text messages would reach school officials and cause a material and substantial disruption inside the schoolhouse, particularly where they were forwarded to a student who was M.Y.'s friend. The student and all adults who read the violent, threatening text messages and depiction of a gun were genuinely distressed.

2. ***Nixon v. Hardin County Bd. of Educ.***, 988 F. Supp. 2d. 826 (W.D. Tenn. 2013)

   Two students, A and B, who disliked each other went to same middle school. They both liked the same boy. A's friend told her that B was with the boy. A and her friend "tweeted" about shooting B in the face and added to their tweet a picture of a face and a gun. The students said the tweets were a joke but conceded that an outsider might not interpret them as a joke.

   The tweets were reported to the school. The Asst. Principal yelled at the students, asking if B deserved this treatment, and A and her friend were assigned to an alternative school for 45 days.

The court denied summary judgment for the school, holding that the speech had no connection to school other than that the students attended there. The speech was not made at school, was not directed to school, and did not involve the use of school time or equipment. No disruption of school activities or environment was shown.

C. Public Employees' Speech

1. Examples of employee Facebook account cases:

***Three D, LLC,* 361 NLRB 31 (2014):** Employer unlawfully discharged two employees for comments posted on their Facebook pages complaining about perceived errors in the employer's tax withholding from their checks. The employer became aware of the posts when showed by another employee who was a Facebook "friend" of the complaining employees. The posts were found to be protected, concerted activity because it was part of a discussion that began in the workplace about the employer's calculation of employee tax withholding. The employees were preparing for group action to encourage the employer to address problems in the terms and conditions of employment. Furthermore, the employer's internet policy that prohibited "inappropriate discussions about the company, management or coworkers" was unlawfully broad because it could be reasonably interpreted to encompass protected activities.

***Richmond District Neighborhood Center,* 361 NLRB 74 (2014):** Employer lawfully rescinded rehire offer to two employees whose Facebook posts were not protected, concerted activity. The Facebook posts, sent to the employer by another employee, included numerous statements advocating insubordination, neglect of duties, and disregard of specific school district rules. The posts undermined leadership and raised safety concerns about their supervision of school district students for whom they provided afterschool activities. The magnitude and detail of the insubordinate acts advocated in the posts gave the employer concern that the employees would act on their plans and a reasonable employer would not risk this action.

2. ***Illinois Right to Privacy in the Workplace Act,*** 820 ILCS 55/10(b) – employer may not demand an employee or employment applicant to provide his/her password to gain access to social media site or demand access to employee's account. However, employer may adopt policy on use of equipment, internet, e-mail and social media.

V. Cyberbullying Update: P.A. 98-0801 (eff. 1/1/15)

A. Amends bullying definition to include "cyber bullying," meaning bullying through the use of technology by e-mail, internet, instant message or fax. It also includes the creation of a webpage in which the creator knowingly impersonates

another person if it creates any effects of bullying or posting and distributing material that creates effects of bullying.

B. Amends bullying statute to include that no student should be subjected to bullying through the transmission of information from a computer that is accessed at a non-school related location or from technology not owned or used by school if the bullying causes a substantial disruption to the educational process or orderly operation of a school. This applies only when a teacher or administrator receives a report that bullying has occurred through this means and does not require a school to monitor a non-school related activity.

C. Anti-Bullying policy must include a process for the district to investigate whether a reported act of bullying is within the permissible scope of the school's jurisdiction. However, nothing in the statute is meant to infringe upon the right to free expression or the free exercise of religion.

VI. Student Records and Other Document Issues

A. **Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices,** PTAC-FAQ-3 (U.S. Dept. of Education Privacy Technical Assistance Center, Feb. 2014)

This Guidance addresses student privacy when a school uses online and cloud services. Information may be shared with an online or cloud service provider, such as Google Docs, Dropbox or iCloud, as a "school official" (i.e. a contractor, consultant, volunteer or other party to whom a school has outsourced services or functions, and who has a legitimate educational interest in the records, so long as information is included in the district's annual FERPA notification to parents).

The online service provider must be under the direct control of the school district with regard to the use and maintenance of the records and must use the records only for authorized purposes. The service provider must refrain from disclosing personally identifiable information in the records without authorization from the school. The district's contract with the online or cloud service provider must include terms concerning use and disclosure of confidential information, the application of FERPA and the school officials exception, the district's ownership of information, data security, data loss, transfer and destruction.

B. **Transparency Best Practices for Schools and Districts,** PTAC-CL-5 (U.S. Dept. of Education Privacy Technical Assistance Center, July 2014)

Schools need to collect a variety of data about students and it is important for schools to communicate with parents what student information they collect, why they collect it, how they use it, how it is protected, and to whom they disclose the data. The district should keep communication lines open with parents, respond timely and thoughtfully and evaluate and improve communication and transparency.

PTAC recommends that a district use its website to communicate about data practices. The website should be user-friendly, searchable and easy to navigate, clear and consistent and reviewed regularly for comprehension and completeness.

C. **Data Destruction**

1. ***Local Records Act,*** 50 ILCS 205

School Districts should maintain a records retention schedule that indicates the retention period for all categories of public records. The records retention schedule must be approved by the Local Records Commission. E-mails that meet the definition of a public record must be retained for the time period set forth in the District's records retention schedule.

2. **Best Practices for Data Destruction,** PTAC-IB-5 (U.S. Dept. of Education Privacy Technology Center May, 2014)

PTAC recognizes data destruction as a critical component of managing data. Methods of destroying data should be based on the risk posed by sensitivity of data and the potential impact of unauthorized disclosure. Include in contracts with third parties that information no longer needed should be destroyed. The contract should ensure accountability for destruction, and indicate how data should be destroyed.

D. ***Personnel Records Review Act*** 820 ILCS 40 – records may be created that an employee has the right to review.

E. Duty to Preserve Evidence in Litigation

A "litigation hold" is when a potential or pending lawsuit involving the District requires the preservation of all records that might be relevant to the lawsuit. Generally, the District receives notice at the beginning of a legal proceeding and is required to identify, locate, and preserve all potentially relevant information, including e-mail messages and metadata. All e-mail messages, without regard to whether they meet the definition of public records, must be retained when the District receives notice of a litigation hold.

***Freeman v. Dal-Tile Corp.,* 750 F.3d 413 (4th Cir. 2014):** Employee brought a suit for hostile work environment and alleged that her employer obstructed justice because it failed to put a litigation hold on all relevant emails upon receipt of the Complaint and destroyed emails pursuant to its retention policy.

F. ***Illinois Freedom of Information Act,*** 5 ILCS 140

***City of Champaign v. Madigan,* 992 N.E. 2d 629 (Ill. Ct. App. 2013):** The City of Champaign denied a FOIA request for copies of electronic communications

sent and received during city council meetings from members of the city council and the mayor. The Illinois Appellate Court held that communications to an individual city council member's *publicly issued electronic device* are subject to FOIA because the device is under the control of the public body. Communications from a city council member's *personal device* are not public records unless they pertain to public business, and were prepared by, used by, prepared for, possessed by, received by, or controlled by the public body. However, if the communication to the personal device is sent or received during the time a city council meeting is in session, it is received while the members are functioning collectively as a pubic body and is a public record subject to FOIA.

VII. Policies

A. PRESS Policy 5:125 Personnel-Personal Technology and Social Media Usage and Conduct

B. PRESS Policy 6:23 Access to Electronic Network

C. PRESS Policy 7:190 Student Discipline

Office\Speeches\PersonalTechIssuesICSA