POTTSGROVE SCHOOL DISTRICT

Technology Department Workshop on Educational Technology Law in a Digital Age

Workshop Objectives:

1. To provide an overview of privacy protections afforded students under federal law and how digital data provides both opportunities for students and challenges to educators.
2. To provide an overview of copyright and fair use doctrine in a digital environment and to distinguish between copyright and licensing provisions for digital content.
3. To provide an overview of student and staff free speech rights and employee privacy rights in school settings.
4. To provide an overview of best practices in safeguarding student and personal data.

Relevant Legislation and Terms and Implications for Students and Educators:

1. Children's Internet Protection Act of 2000 (CIPA) with subsequent FCC rule changes such as Protecting Children in the 21st Century Amendment 2012
2. Children's Online Privacy Protection Act of 1998 and subsequent FTC rule changes (COPPA)
3. Family Educational Rights and Privacy Act of 1974 (FERPA)
4. Federal Rules of Civil Evidence
5. Pennsylvania Information Management System (PIMS)

Relevant District Policies

1. 815.1 – Acceptable Use…
2. 816 – Use of Social Media

CIPA

What CIPA requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

Source – Federal Communications Commission

COPPA

Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012. The amended Rule took effect on July 1, 2013.

The primary goal of COPPA is to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13 while accounting for the dynamic nature of the Internet. The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.

Operators covered by the Rule must:

1. Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
2. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
3. Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
4. Provide parents access to their child's personal information to review and/or have the information deleted;
5. Give parents the opportunity to prevent further use or online collection of a child's personal information;
6. Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and
7. Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.

Source – Federal Trade Commission

<u>FERPA</u>

FERPA affords student (or parent if a student is a minor) access to educational records and to challenge the contents of that record.

Under FERPA, a school may not generally disclose personally identifiable information from an eligible student's education records including discipline records to a third party unless the student or parent if student is a minor has provided written consent. However, there are a number of exceptions to FERPA's prohibition. Under these exceptions, schools are permitted to disclose personally identifiable information from education records without parental or student consent, though they are not required to do so. There are many exceptions. Here are a few:

- Certain legitimate research purposes
- Compliance with a court order or other judicial matters
- Directory information including name address, phone, activities, photo, etc. (parent/student may opt out)

- School officials including teachers, but not defined in law, with a legitimate need to know to perform their official function
- Certain third parties performing specific task on behalf of the school district

Source - Federal Department of Education

Excerpt from Board Policy 815.1

Privacy and Security

1. FERPA gives parents/guardians and eligible students the right to request that certain information not be made public. Therefore, some may elect to not have student contact information (such as, e-mail addresses) published in District public directories or communicated beyond the District's network or e-mail system or course setting.

2. No specific personal or personally identifiable information shall be released to any individual over the telephone, by e-mail or voice mail message. Directory information may be released, if it does not invade the privacy of the student, however, if the parent/guardian has indicated on the annual Directory Information Notice that no information may be released for their child no such information may be disclosed. Directory information may include the student's name, degrees and awards received, participation in officially recognized activities or sports. Other uses of e-mail includes obtaining homework and instructional material, explaining work and homework, asking for information and references, obtaining lost handouts or assignment sheets and explaining absences.

3. Other people can read your e-mail while it is in transit, and the recipient can transfer the e-mail message to those s/he chooses.

4. E-mail, chat rooms, electronic bulletin boards, text messaging and other electronic communications are not appropriate for transmitting sensitive or confidential information. Confidentiality for such messages is protected by FERPA, and other privacy laws such as HIPAA and PPRA *(Protection of Pupil Rights Amendment limiting a school's right to survey students on certain topics considered sensitive without full disclosure and permission from parents and administered by the Federal Dept. of Ed.).*

5. All use of e-mail must be consistent with the District's Student Record's Policy and Plan. Remember that the recipient has the right to redirect (forward) or share your message with others. You are responsible for ensuring that the message is accurately sent and the message is sent at your own risk.[3]

6. You must include in the e-mail subject line and leading lines of the body of the e-mail text "CONFIDENTIAL – (__Insert Student's Name__. DO NOT DISCLOSE OR REDISCLOSE)." See attached Parent/Guardian Consent for a Student's Personally Identifiable Information to be sent by electronic mail form.

7. When you find that it is necessary to provide information in an e-mail that has personally identifiable information, you should speak in general terms, i.e., explain policies and/or procedures for situations without confirming or denying personal information. (Think Federal Rules of Civil Evidence)

One other note: The practice of using student initials instead of a student name in an email has no practical value. The email may still be deemed an educational record (think FERPA), may still be held in the case of potential litigation (think Rules of Civil Evidence), and may only serve to make the District's search process more difficult.

Access and Security Prohibitions

Users must immediately notify the Director of Technology and/or designee if they have identified a possible security problem. Students, employees, and guests must read, understand and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure and physical information security policies. The following activities related to access to the District's CIS systems, and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Acquiring or attempting to acquire passwords of others or giving your password to another. Users will be held responsible for the result of any misuse of the users' user name or password while the users' systems access were left unattended and accessible to others, whether intentional or through negligence.

3. Using or attempting to use computer accounts of others, these actions are illegal, even with consent, or if only for the purpose of "browsing".

4. Altering a communication originally received from another person or computer with the intent to deceive.

5. Using District resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity of any kind, or being involved in a terroristic threat against any person or property,

including cyber bullying.

6. Disabling or circumventing any District security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.

7. Transmitting electronic communications anonymously or under an alias unless authorized by the District.

Search & Seizure

8. User's violations of this policy, any other District policy, or the law may be discovered by routine maintenance and monitoring of the District system, or any method stated in this policy, or pursuant to any legal means.

9. The District reserves the right to monitor, track, log and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason. Users should not have the expectation of privacy in their use of the District CIS systems, and other District technology, even when used for personal reasons. Further, the District reserves the right, but not the obligation, to access any **personal technology device of users brought onto the District's premises or at District events, or connected to the District network, containing District programs or District or student data (including images, files, and other information) to ensure compliance with this policy and other District policies, to protect the District's resources, and to comply with the law.**

10. **Everything that users place in their personal files should be written as if a third party will review it. (Think Federal Rules of Civil Evidence)**

Copyright Infringement and Plagiarism

11. **Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the District resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements and employees will respect and comply as well.**

12. **Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The District does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.**

13. Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the District's computers is expressly prohibited. This includes all forms of licensed software – shrink wrap, click wrap, browse wrap, and electronic software downloaded from the Internet.

14. District guidelines on plagiarism will govern use of material accessed through the District's CIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

Copyright is assumed unless there is a disclosure of public domain. Avoid using registered trademarks on your web pages.

http://www.pbssocal.org/education/teachers/copyright/ is a great site with informational videos for teachers and administrators, quizzes, and other materials.

https://creativecommons.org/licenses/ is an alternative to "All Right Reserved" traditional copyright and used to maintain ownership of digital content but to allow certain kinds of sharing in non-commercial settings with attribution.

Fair use of videos in classrooms must meet the following criteria:

1. Content must advance learning of the established curriculum.
2. The video must be legally obtained.
3. It must be shown in the classroom with the rostered students and instructor of record.

Videos streamed from personally subscribed commercial sources such as Netflix may qualify under the criteria above but still have home use of streaming technology licensing restrictions in place.

Fair use is NOT intended to deny the owner of content revenue from his/her work.

Fair use does NOT apply to works being "broadcast" over Internet or other media.

Excerpt from Board Policy 816

Examples of electronic communications in which staff members are prohibited to engage include, but are not limited to:

1. Sending communications to students that are not related to the overall mission of the district.

2. Providing a staff member's personal cell phone number to students, except under limited circumstances, as part of a district-sponsored activity, and with prior approval from the staff member's supervisor.
3. Placing a phone call to a student's personal cell phone, except under limited circumstances, as part of a district-sponsored activity, and with prior approval from the staff member's supervisor.

4. Sending SMS/text messages to students, except under limited circumstances, as part of a district-sponsored activity, and with prior approval from the staff member's supervisor.

5. E-mailing students from a staff member's personal email account.

6. Providing students with a staff member's personal email (non-district provided) account/address.

7. "Friending" or otherwise adding students to their circle of contacts on an online social networking site whose function does not involve enhancing the educational goals of the district.

8. Publically displaying or posting online material that would be disruptive to the educational process, including, but not limited to provocative statements, provocative photographs, and/or other public or online activities that would jeopardize the professional nature of the staff-student relationship.

9. Discussing situations involving employee or student discipline in electronic forums or use of social media in a manner that interferes with the employee's work obligations or impacts upon another staff member's effectiveness within the school system.

10. Using any district device or network to send or attempt to send a communication anonymously or in any manner so as to disguise the identity of the actual sender.

11. Representing personal opinions as those of the district.

12. Using any district device or network to upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the district, or the district itself.

13. Revealing or publicizing confidential or proprietary information.

14. Disclosing personally identifiable information related to a student, except in strict accordance with Board Policy and the Family Educational Rights and Privacy Act and the regulations promulgated there under.

15. Using any district device or network to facilitate or participate in blogging, unless used for a clear educational purpose and otherwise consistent with law and Board Policy.

16. Using any district device or network to participate in or facilitate chat rooms unless used for a clear educational purpose and otherwise consistent with law and Board Policy.

17. Using any district device or network to download files, games, music or video, unless, for a clear educational purpose, or under the limitations of employee personal use as set forth in Policy 815.1 and always in accordance with Copyright and Fair Use Guidelines.

18. Sharing passwords to district operated systems with or allowing passwords to district operated systems to be used by anyone else.

Staff members are encouraged to use a district provided means of communication (e.g. district e-mail, district phone) when contacting students. However, emergency circumstances may arise that require a staff member to communicate with a student via a non-district provided method of communication. In such an instance, it is the responsibility of the staff member to report such situations to their supervisor at the first opportunity.

<u>Protect Your Data and Your Students' Data</u>

1. Never put anything in an email you don't want to answer for under oath.
2. Most hacks are low tech. Passcodes are supposed to be inconvenient. Don't leave them where others can see them.
3. Good passcodes should be alphanumeric with capital and lowercase letters, as well as special symbols. Make it meaningful, however, to help you remember it.
4. Don't have one passcode for all occasions.
5. Never allow students or others not authorized to access district and student data to use your district-issued laptop and iPad.
6. Know the privacy settings on social media and keep them tight.
7. Never reveal personal information via email or social media
8. Use an alternative email address for commerce and social media
9. Select a security question that is difficult for someone to look up. For example, your mother's maiden name or your high school mascot are probably not good choices.

10. Try to keep work files off of personal computers and vice versa (this does not preclude incidental personal use)
11. Know and abide by our social media policy, as it is designed to protect you, the students, and the District.
12. Look at privacy policies, customer loyalty cards, etc. and you decide how much you are willing to reveal about yourself. However, what you reveal about students is restricted under law and District policy.