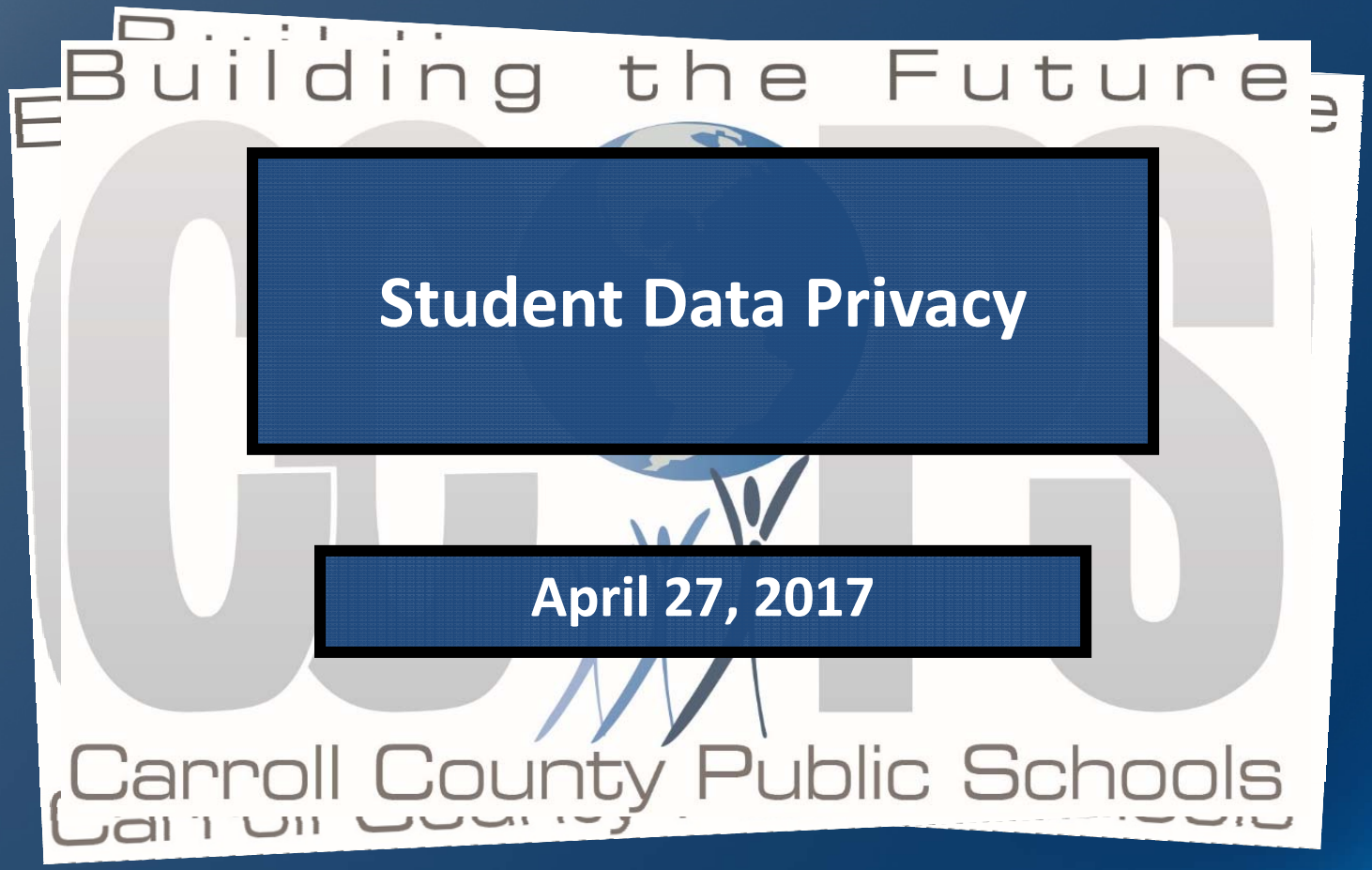


Student Data Privacy

April 27, 2017

Purpose and Desired Outcomes

Purpose: To clarify system expectations and roles for review of Third Party Vendor's Terms of Service, Privacy Policies, and/or End User License Agreements.

Desired Outcomes: By the end of the session, we will have:

- An understanding of staff roles in the approval of Technology Applications requested to be used in CCPS classrooms;
- An understanding of the federal requirements and best practices related to the review of agreements;
- An understanding of the Maryland and CCPS expectations related to the review of agreements.

Staff Roles in the Approval Process

- Current Workflow:
  - Teachers
  - Content Supervisor
  - Instructional Technology Review Team
    - Curriculum Staff
    - Supervisor of Research and Accountability
    - Technology Staff
  - Additional Staff (Special Education and Student Services)

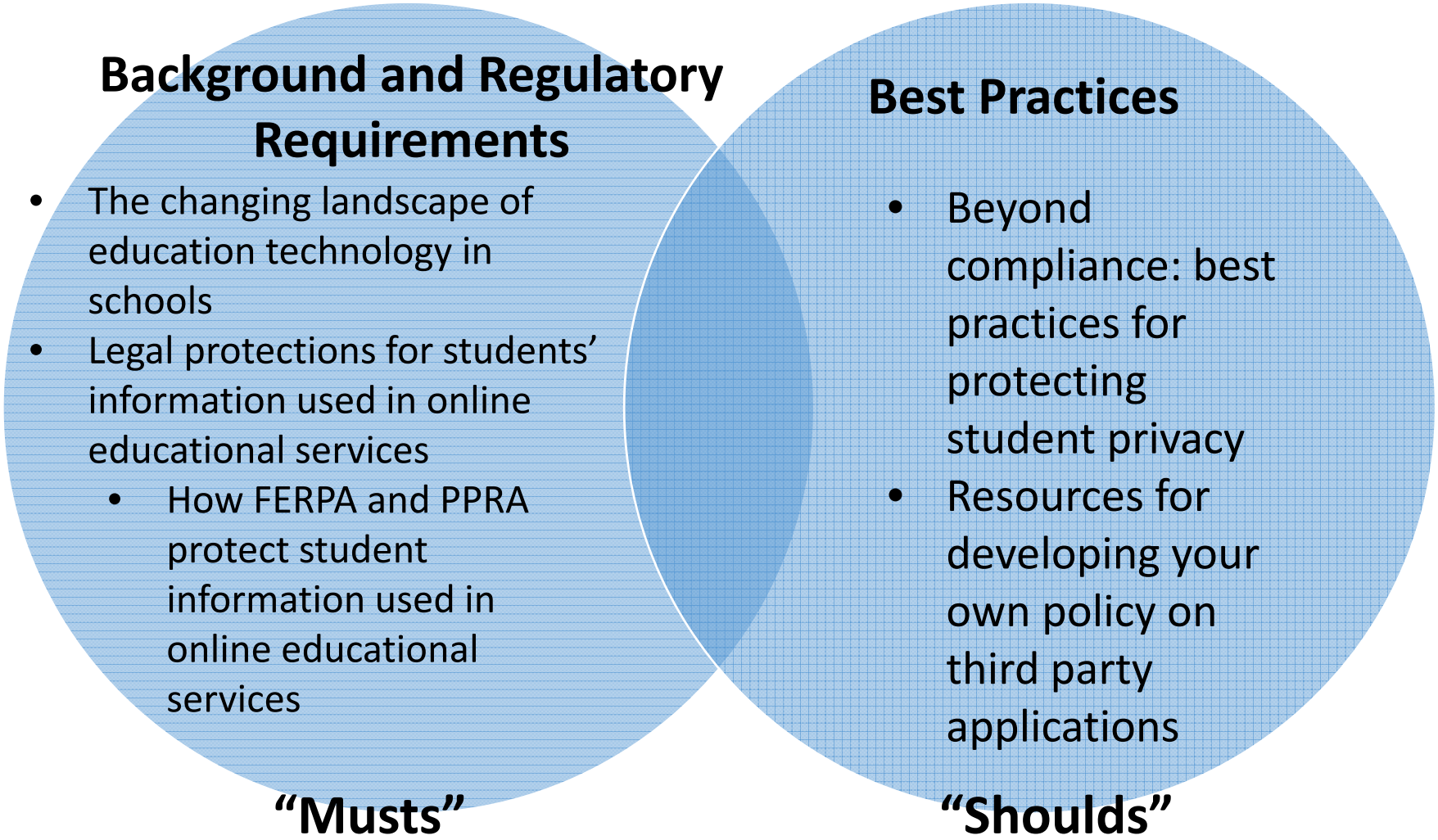
Carroll County Vetting Apps for the Classroom Discussion

April 2017

BARON RODRIGUEZ
Privacy Technical Assistance Director

United States Department of Education
Privacy Technical Assistance Center

Summary of Today's Discussion



Online Educational Services

This guidance relates to the subset of education services that are:

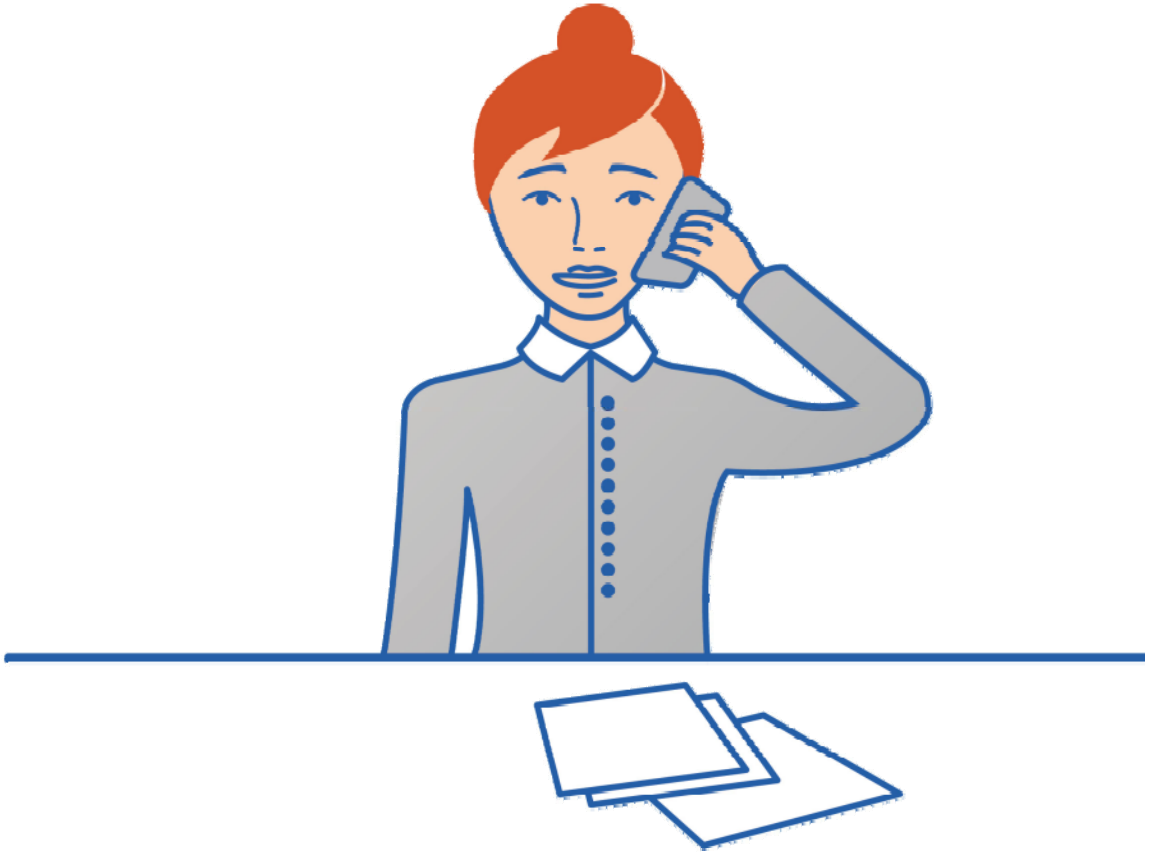
- Computer software, mobile applications (apps), or web-based tools;
- Provided by a third-party to a school or district;
- Accessed via the Internet by students and/or parents; AND
- Used as part of a school activity.

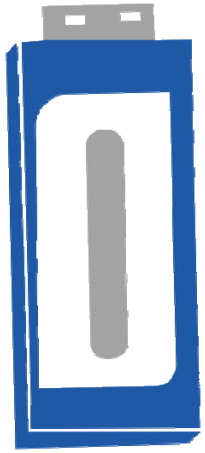
**This guidance does not cover online services or social media used in a personal capacity, nor does it apply to services used by a school or district that are not accessed by parents or students.*

The Challenge of Online Educational Services

- Schools and districts are increasingly contracting out school functions
- We have new types of data, and much more of it!
- Many online services do not utilize the traditional 2-party written contractual business model
- Increasing concern about the commercialization of personal information and behavioral marketing
- We need to use that data effectively and appropriately, and still protect students' privacy

Let's test your data security posture!





Android Best Practices

- The best thing you can do to protect against Android mobile application vulnerabilities and malware is to educate users about access permissions after installing a mobile application. User approval is required before any app can access other data or apps on an Android device. Just as you train users not to open strange email attachments, they should be equally cautious with requests from apps to access data they shouldn't need access to.

But I-Phone's are secure!!!

Well…

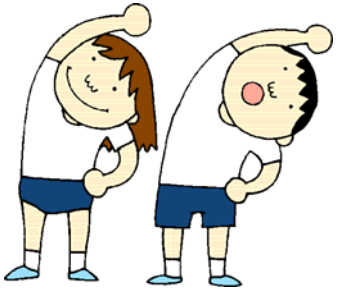
- Mobile application vulnerabilities are not limited to Android apps. A mobile application called Path, for example, offered a new way to socialize with friends and was hailed for its great user interface. Then someone sniffing the network activity of the app revealed that Path uploaded entire contact lists to its servers. It did not ask permission to do so in the iOS version of the app. Path had to apologize for unauthorized storage of users' personal data.

And… just a while ago…

- iPhone owners should now take note: a security researcher today warned there are comparable vulnerabilities to those Stagefright bugs in iOS allowing completely silent, almost undetectable password theft from iPhones. Apple has patched the flaws in iOS 9.3.3, however, and users have been advised to update as soon as they can.

Source:
http://www.forbes.com/sites/thomasbrewster/2016/07/19/apple-iphone-ios-9-vulnerabilities-like-stagefright/#8393ec139476

What about health apps?



- A 2016 Mobile Apps Study underscores the necessity of strong Best Practices for health and wellness data.
  - The App Study revealed that health and fitness apps generally do worse than average at providing privacy policies. Only 70% of top health and fitness apps had a privacy policy (6% lower than overall top apps), and only 61% linked to it from the app store listing page (10% lower than overall top apps).

So… you *still* want to know about using downloading "free" apps in the classroom?

What does FERPA require if PII is disclosed to a provider?

- Parental consent for the disclosure; OR
- Disclosure under one of FERPA's exceptions to the consent requirement. Typically, either:
  - Directory Information exception
    - Remember parents' right to "opt-out"
  - School Official exception
    - Annual FERPA notice
    - Direct control
    - Use for authorized purposes only
    - Limitation on re-disclosure
    - *Remember parents' right to access their student's education records*

Question

Under FERPA, are providers limited in what they can do with the student information they collect or receive?

Are providers limited in what they can do with the student information they collect or receive?

If PII is disclosed under the Directory Information exception:

- No limitations other than what the school/district includes in their agreement with the provider.

If PII is disclosed under the School Official exception:

- PII from education records may only be used for the specific purpose for which it was disclosed
- TPPs may not sell or share the PII, or use it for any other purpose except as directed by the school/district and as permitted by FERPA

When personal information is collected from a student, the PPRA may also apply!

- *PPRA places some limitations on the use of personal information collected from students for marketing*

Question:

What about metadata? Are there restrictions on what providers can do with metadata about students' interactions with their services?

What about metadata?

"Metadata" are pieces of information that provide meaning and context to other data being collected, for example:

- Activity date and time
- Number of attempts
- How long the mouse hovered before clicking an answer

Metadata that have been stripped of all direct and indirect identifiers are not protected under FERPA (note: school name and other geographic information are often indirect identifying information in student data)

Properly de-identified metadata may be used by providers for other purposes (unless prohibited by their agreement with the school/district)

Other laws to consider

- Children's Online Privacy and Protection Act (COPPA)
  - Applies to commercial Web sites and online services directed to children under age 13, and those Web sites and services with actual knowledge that they have collected personal information from children
  - Administered by the Federal Trade Commission
  - See http://www.business.ftc.gov/privacy-and-security/childrens-privacy for more information
- State, Tribal, or Local Laws

COPPA BACKGROUND

- Statute enacted in 1998, Rule revised in 2012

- Goals
  - Allow parents to make informed choices about when and how children's personal information is collected, used, and disclosed online.
  - Enable parents to monitor their children's interactions and help protect them from the risks of inappropriate online disclosures.

Basic Requirement

- Operators of commercial websites, apps, and online services must provide NOTICE and obtain parental CONSENT before collecting personal information from children under age 13.
  - All websites and online services operated by the Federal Government and contractors operating on behalf of federal agencies must comply with COPPA. See *OMB Guidance for Implementing Privacy Provisions of the E-Government Act of 2002* (Sept. 2003)

COPPA Applies to…

- Child-directed sites and services.
- General audience sites with actual knowledge they're collecting personal information from kids under 13.
- Third parties with actual knowledge they're collecting personal information directly from users of a service directed to children.

"Collects or collection"

- Requesting, prompting, or encouraging that children submit personal information online, even when optional.
- Enabling children to make the information public, *e.g.*, in a chat room or profile.
- Passive tracking linked to personal information.

Under COPPA, operators must:

- Notice
  - Post a privacy policy and links to the policy wherever personal information is collected.
  - Give parents direct notice of its information practices.

- Consent
  - With certain exceptions, obtain verifiable parental consent before collecting information.

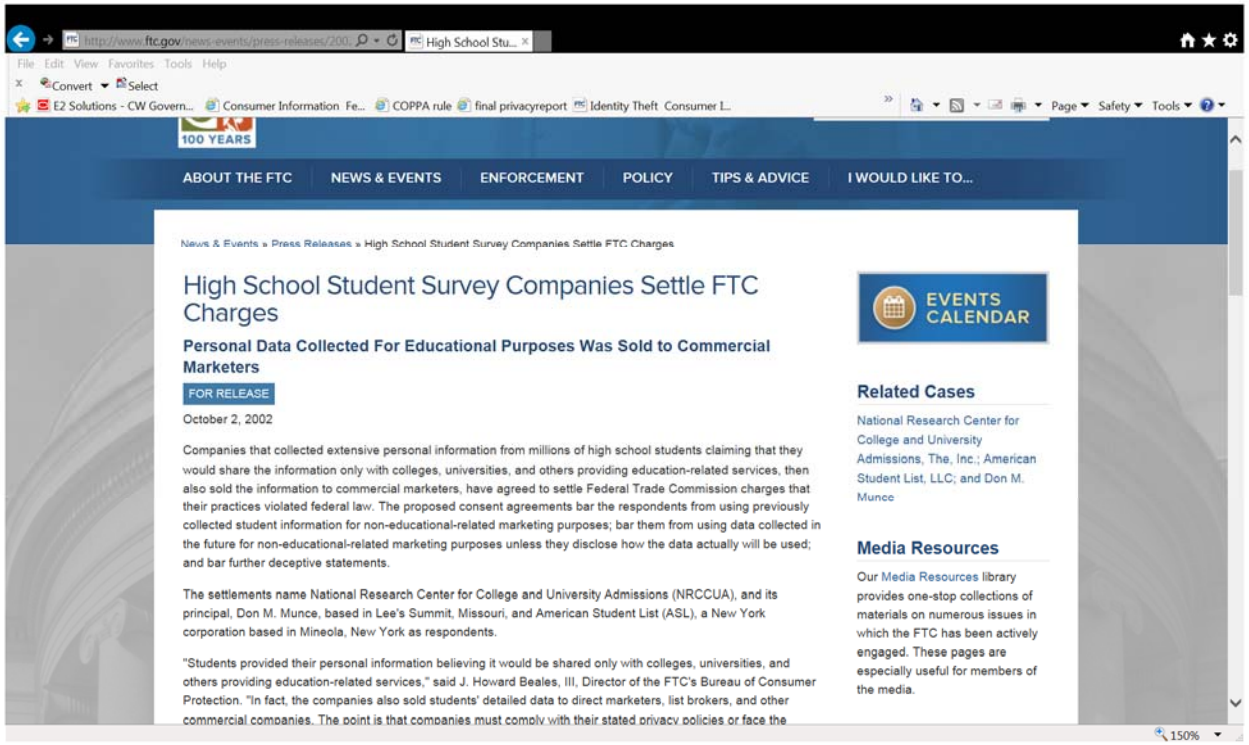
COPPA and Schools

- Can operators get consent from schools instead of parents to collect personal information from students?
  - Yes if for the use and benefit of the school and no other commercial purpose.
  - Teacher, school, district? Best practice is go through school or district.

FTC Act Enforcement

- Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”
- Deception: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.
- Unfairness: practices that cause or are likely to cause substantial injury to consumers that are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers.

Section 5 in schools



STUDENT PRIVACY PLEDGE

- More than 300 companies have signed on to the student privacy pledge, which makes clear that the school service providers will:
  - Not sell student information;
  - Not behaviorally target advertising
  - Use data for authorized education purposes only
  - Not change privacy policies without notice and choice
  - Enforce limits on data retention
  - Support parental access to, and correction of errors in, their children's information
  - Provide comprehensive security standards
  - Be transparent about collection and use of data

For companies signing on, failure to do so may be a deceptive trade practice under the FTC Act

Common COPPA Mistakes

- Privacy Policy must include all operators collecting personal information on your site
- Link must be on home or landing page and at each area of the site or service where personal information is collected. If a general audience site with a children's portion, you must directly link to the children's portion on those child directed portions of the website.
- Your direct notice may not simply link to privacy policy
- Collecting date of birth on general audience site and then failing to obtain parental consent from those with birth dates showing they are under 13
- Collection of photos or audio from children and not considering personal information. Relatedly, many photos contain geolocation
- Child-directed sites strictly liable for information collection on their sites/services by third parties

RESOURCES

- FTC's Business Center: www.ftc.gov/tips-advice/business-center/privacy-and-security

- COPPA FAQs: www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Questions

Protection of Pupil Rights Amendment (PPRA)

- Amended in 2001 with No Child Left Behind Act
- Mostly known for its provisions dealing with surveys in K-12
- Includes limitations on using personal information collected from students for marketing
- May require parental notification and opportunity to opt out
- May require the Development of policies in conjunction with parents
- However … a significant exception for "educational products or services"

Best Practices for Protecting Student Privacy

- **Maintain awareness of other relevant laws**
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- **Be aware of which online educational services are currently being used in your district**
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- **Have policies and procedures to evaluate and approve proposed educational services**
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Question:

Can individual teachers sign up for free (or "freemium") education services?

Using free or "freemium" educational services

Remember the FERPA's requirements for schools and districts disclosing PII under the school official exception.

- Direct control
- Consistency with annual FERPA notice provisions
- Authorized use
- limits on re-disclosure

These services may also introduce security vulnerabilities into your school networks!

It is a best practice to establish district/school level policies governing use of free/freemium services, and to train teachers and staff accordingly.

Ask yourself this question:

- Can your teachers enter into a legally binding contract on behalf of the district?
  - If the answer is no….
  - If the answer is yes…

Regardless of your answer!

- Every school or district should have a policy in place for reviewing agreements before the service or application is used in the classroom.
  - Schools/Districts should establish a review process and/or have a designated individual review TOS before its adoption.
  - The service or application should be inventoried, evaluated, and support the school's and district's broader mission and goals.

Click-Wrap Agreements

- These agreements are referred to as "click-wrap" agreements, and can operate as a provider's legally-binding contract.
- Once a user at your school or district clicks "I agree," the terms of this agreement will likely govern what information the provider may collect from or about students and with whom they may share it.

Click-Wrap Agreements (cont'd)

- Click-Wrap agreements could potentially lead to a violation of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), or other laws, as well as privacy best practices.

Privacy-Related TOS Provisions

- We'll now begin discussing example provisions from TOS

- The example provisions are intended to give you a general idea of what to expect when reviewing a TOS
  - Please keep in mind that specific language will vary from TOS to TOS

Data De-Identification

- There is a significant amount of data available to providers of educational services.
  - Metadata on students' interaction with the service or app is often collected and analyzed to help improve the product and enable a provider to create more effective educational services.

Data De-Identification (cont'd)

- Even stripped of identifiers, student data could still be identifiable (through demographic or contextual information collected by the app, or through information available elsewhere).

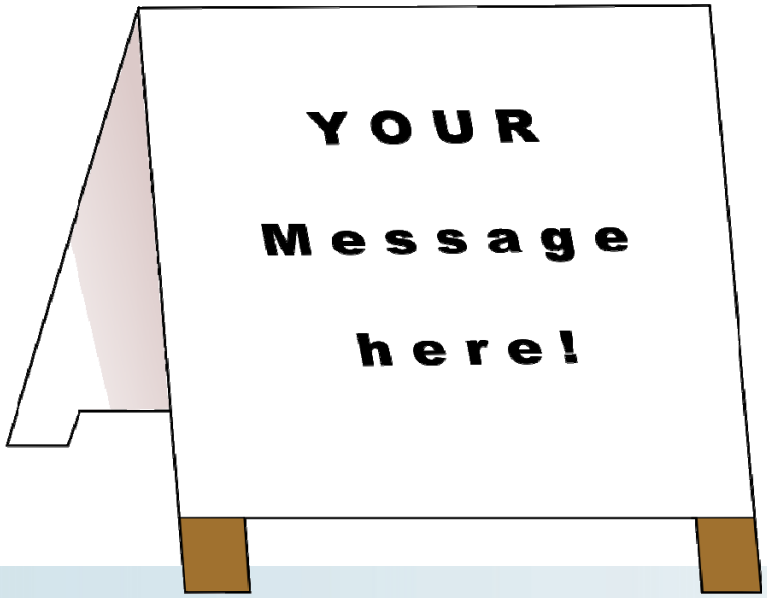
Marketing and Advertising

- Information gathered in an online educational service or mobile application could be used to create a profile on a student.

- That profile could then be used to direct advertising/marketing materials to students.

Marketing and Advertising (cont'd)

- The language in a TOS should be clear that the data collected cannot be used to advertise or market to students.
  - Targeted advertising/marketing could violate privacy laws.



Data Mining

- Providers often perform "data mining" on information they collect to identify patterns in the data, or to infer additional information about their users.
  - Data Mining: the practice of examining large databases in order to generate new information

Google
Apps for Education

Security Controls

- Student data need to be protected, and a provider's TOS should include provisions outlining strong policies safeguarding those data.
- Failure to provide adequate security could lead to a FERPA violation.

Best Practices for Contract Provisions for Online Educational Services (See Website!!)

- Security and data stewardship provisions
- Data collection provisions
- Data use, retention, disclosure, and destruction provisions
- Data access provisions
- Modification, duration, and termination provisions
- Indemnification and warranty provisions

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

http://ptac.ed.gov

(855) 249-3073

PK LAW

Student Data Privacy – Clarification of Expectations and Roles

Board of Education of Carroll County

Presented by ***Adam E. Konstas, Esq.***

Pessin Katz Law, P.A.

PK LAW®

Topics

- Future of Privacy Forum's Student Privacy Pledge
- Maryland Student Data Privacy Act of 2015
- Carroll County Public Schools Policy, Administrative Regulation, and Procedure
  - Policy AF: Student Data Privacy
  - Administrative Regulation AF
  - Standard Operating Procedure A1

PK LAW®

Tammy Teacher's Monday Morning Class . . .

- One Saturday afternoon, Tammy Teacher discovers a web-app that she thinks would be perfect for her classroom opening exercises on Monday morning. Tammy Teacher downloads the app and clicks "I Agree" to the terms of service. Tammy sends a link to the app to her students to download so they can participate in the exercise Monday morning.
- At the beginning of class, Tammy Teacher prompts her class to respond to a quiz using the new app she found. Students submit their responses to the quiz through the app and the results are generated on a screen in front of the class.
- The opening exercise is a big success! The students learned a lot, the teacher found the app useful, and everyone in the classroom cannot wait to use the app again.

PK LAW®

The Very Next Day . . .

- The IT department finds out that Tammy Teacher downloaded the app and directed her students to download the app.
- Parents find out that their students are working on a new app in the classroom.
- Parental concerns/Admin concerns/Board concerns

PK LAW®

The District's Response . . .

- Is there a problem here?
- How do we make sure that this does not happen again?

- Technology is an integral part of a 21st century education.
- There is no going back. So, how to we utilize technology safely, manage risks, and prepare our students for college and careers?

PK LAW®

Student Privacy Pledge

- In October of 2014, the Future of Privacy Forum and the Software & Information Industry Association introduced a "Student Privacy Pledge" to safeguard student privacy regarding the collection, maintenance and use of student personal information.
- In January 2015, President Obama strongly endorsed the pledge.
- The Pledge contains a dozen key commitments by major service providers and articulates a set of expectations that parents and school officials should have about their students' data.
- https://studentprivacypledge.org/

PK LAW®

Student Privacy Pledge

- There are 328 signatories to the pledge, and counting . . .
- Some of the signatories to the Pledge include:
  - Apple
  - Google
  - Brainpop
  - Edmodo
  - College Board
  - Blackboard
  - Microsoft

PK LAW®

Student Privacy Pledge

- We pledge to carry out responsible stewardship and appropriate use of student personal information according to the commitments below and in adherence to all laws applicable to us as school service providers.
- We Commit To:
- ✗ Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- ✗ Not sell student personal information.
- ✗ Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.
- ✗ Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.
- ✗ Not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data is used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements.
- ✗ Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.

PK LAW®

Student Privacy Pledge

- ✓ Collect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution/agency, teacher or the parent/student.
- ✓ Disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information we collect, if any, and the purposes for which the information we maintain is used or shared with third parties.
- ✓ Support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent.
- ✓ Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.
- ✓ Require that our vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information.
- ✓ Allow a successor entity to maintain the student personal information, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

PK LAW®

Student Privacy Pledge

- **Notes:**
  - Some school service providers may be subject to additional legal obligations, contractual commitments, or requests from educational institutions or parents/students that direct or otherwise authorize additional uses of student data, other than those specified above.
  - Nothing in this pledge is intended to prohibit the use of student personal information for purposes of adaptive learning or customized education.
  - This pledge is intended to be applicable to new contracts and policies going forward and addressed — where inconsistent and as agreed to by the educational institution or agency — in existing contracts as updated over time.
  - This pledge shall be effective as of January 1, 2015.
- **Definitions:**
  - 'School service provider' refers to any entity that: (1) is providing, and is operating in its capacity as a provider of, an online or mobile application, online service or website that is both designed and marketed for use in United States elementary and secondary educational institutions/ agencies and is used at the direction of their teachers or other employees; and (2) collects, maintains or uses student personal information in digital/electronic format. The term 'school service provider' does not include an entity that is providing, and that is operating in its capacity as a provider of, general audience software, applications, services or websites not designed and marketed for schools.
  - 'Educational/School purposes' are services or functions that customarily take place at the direction of the educational institution/agency or their teacher/employee, for which the institutions or agency would otherwise use its own employees, and that aid in the administration or improvement of educational and school activities (e.g., instruction, administration, and development and improvement of products/services intended for educational/school use).
  - 'Student personal information' is personally identifiable information as well as other information when it is both collected and maintained on an individual level and is linked to personally identifiable information.
  - 'Student' applies to students of United States elementary and secondary schools, and with regard to notice and consent applies only to students of appropriate age as authorized under relevant United States federal law.
  - 'Consumer privacy policies' include those privacy policies that are posted by the company to be available to all users to the site or service.
  - 'Parent' includes a student's legal guardian.

PK LAW®

Maryland Student Data Privacy Act of 2015

- Md. Code Ann. Educ. § 4-131
- **Covered information**: name, address, phone number, email, test results/grades, medical records, SSN, other indirect identifiers
- **Operator**: person who is operating in accordance with contract of agreement with public school or local school system in the state to provide an internet web site, online service, online app, or mobile app that is:
  - used primarily for a PreK-12 purpose
  - Is issued at direction of public school, teacher, school system employee
  - Was designed and marketed primarily for a PreK-12 purpose

PK LAW®

Maryland Student Data Privacy Act of 2015

- Requires operators of specific websites, online services, online apps, mobile apps, designed primarily for preK-12 public school purposes, operating according to a contract to:
  - Protect covered information from unauthorized access, destruction, use, modification.
  - Implement and maintain reasonable security measures
  - Delete covered information upon request of school system

PK LAW®

Maryland Student Data Privacy Act of 2015

- Operator may not knowingly:
  - Engage in targeted advertising based on data collected through website, service, app, etc.
  - Except in furtherance of school purpose, use information to make a profile about a student
  - Sell a student's information
  - Disclose covered information
- Operator may use aggregated or de-identified information under certain circumstances
- Does not apply to general audience websites

PK LAW®

Carroll County Public Schools

Policy AF: Student Data Privacy

Definitions:

- **Technology Applications** – Includes all computers based and online educational resources used by Carroll County Public Schools (CCPS) students and staff.
  - Compare with Maryland Law's definition of "Operator" – The CCPS definition is somewhat broader.
- **Personally Identifiable Information** – Personally identifiable information includes the student's name, address, telephone number, social security number, or other personally identifiable information. For the purposes of this procedure, personally identifiable information has a meaning consistent with its meaning under the Family Education Rights and Privacy Act (FERPA).
  - Compare with Maryland Law's definition of "Covered Information" and FERPA's definition of "Personally Identifiable Information"
  - The CCPS definition is meant to be consistent with State and Federal law.

PK LAW®

Carroll County Public Schools

Policy AF: Student Data Privacy

Policy Statement:

- Technology applications, including online educational services, are recognized as a viable educational tool to create, share, store, distribute and manage student work. These tools can be accessed by students and/or parents and used as a part of the school's educational program in or outside of the school day. **While CCPS encourages the use of educational technological advancement in the furtherance of its educational mission, no educational tool that compromises protected personally identifiable information on students shall be permitted**.

- Note: There is a delicate balance between the utility of online services as educational tools and the risk of disclosure of student PII.

PK LAW®

Carroll County Public Schools

Administrative Regulation AF

Two key committees:

1. Instructional Technology Resource Team
2. Technology Review Board

Purpose: Provide oversight, expertise, responsibility for student data privacy policy and procedures, maintain consistency throughout district.

PK||LAW®

Carroll County Public Schools

Administrative Regulation AF

- Who has authority to approve technology application contracts?
  - Superintendent
  - Supervisor of Purchasing
  - Assistant Superintendent of Administration
  - Supervisor of Research and Accountability
- Did Tammy Teacher sign a contract?
  - YES . . . "Tammy Teacher downloads the app and clicks 'I Agree' to the terms of service."

PK||LAW®

Carroll County Public Schools

- Remember . . .
  - The use of technology applications is **optional**. No parent or student shall be required by CCPS to sign user rights agreement.
  - Consent form for parent/guardian permission for use of technology applications that required disclosure of student PII and/or acceptance of user agreement.
  - Parent/guardian may request alternative classroom resources be used.
- What does this mean?
  - Consider alternative means of instructional delivery.
  - Consider utility of tool in the first place . . . What purpose does the tool serve as a part of the lesson? Distinguish meaningful use of tool from gratuitous use.
  - Do students feel compelled to use tool or do they truly feel that the tool is optional?

PK LAW®

Carroll County Public Schools

What if the technology application requires the submission of student PII and/or acceptance of user agreement?

- Any technology application that requires the **submission of students' personally identifiable information and/or acceptance of a user agreement must be approved by the Instructional Technology Resource Team** prior to use.
- Employees are expected to follow state and federal laws governing student data privacy.
- No employee or third party may claim ownership/property/copyright rights to student work product
- Third party vendors who collect student PII must provide assurances of compliance with the Maryland Student Data Privacy Act of 2015.

PK LAW®

Carroll County Public Schools

What if the technology application **does not** require the submission of student PII and/or acceptance of user agreement?

- Classroom teachers are permitted to use these technology applications as long as such use is consistent with the mission and objectives of the Carroll County Public School System and complies with all applicable laws.

PK LAW®

Carroll County Public Schools

The Instructional Technology Resource Team Review

The ITRT's internal procedures shall have in place management, operational, and technical security controls to protect the school system from a breach of student data. For technology applications that require PII student data, these procedures shall include, but not be limited to:

a. A prohibition against the vendor's **secondary use of student data** including sales, marketing or advertising;

b. A prohibition against the vendor's **modification of the contract without advanced notice and consent**;

c. A requirement that the vendor **limit data collection and use for the purpose of fulfilling its duties** as outlined in the user agreement;

d. A prohibition **against mining data for any purposes other than those stated in the agreement**;

e. A requirement to **de-identify PII for any use of data for product development, research or other purposes**;

f. A prohibition against **sharing PII without prior written consent** of the user except as required by law;

g. An assurance that all **PII student data in a vendor's possession shall be destroyed or transferred to CCPS after the data is no longer needed**;

h. A requirement that any **PII on students be made available to CCPS upon request**;

i. A requirement that the vendor have in place **management, operational, and technical security controls** in accordance with industry best practice to protect from a data breach;

j. A requirement that the vendor has **limited, nonexclusive license** to CCPS and student intellectual property, content, and data for the **sole purpose of performing its obligations** as outlined in the agreement; and

k. A requirement that the vendor agree to **comply with all applicable state and federal laws**.

NOTE THAT THESE REQUIREMENTS ARE CONSISTENT WITH THE COMMITMENTS OF THE STUDENT PRIVACY PLEDGE AND MARYLAND STUDENT DATA PRIVACY ACT

PK LAW®

Carroll County Public Schools

The Instructional Technology Resource Team Internal Procedures

The ITRT's internal procedures shall have in place management, operational, and technical security controls that would prohibit the approval of terms of use agreements that:

a. Allow for secondary use of data for marketing, sales, and targeted advertising to users of the service;

b. Claim that intellectual property rights related to the content that is uploaded or created by the user will be owned by the service;

c. Contain content that is objectionable and/or does not serve an instructional purpose;

d. Contain services that require the release of FERPA-protected information

NOTE THAT THESE REQUIREMENTS ARE CONSISTENT WITH THE COMMITMENTS OF THE STUDENT PRIVACY PLEDGE AND MARYLAND STUDENT DATA PRIVACY ACT

PK LAW®

Carroll County Public Schools

Guidelines for Parents and Students

- Use technology applications as directed by CCPS teachers and staff
- Use only your registered account
- You are responsible for the proper use of your registered account
- Keep personal account information private
- Follow acceptable use policies and procedures
- Users shall not intentionally upload, download, or create computer viruses or maliciously attempt to harm or destroy district equipment or materials or hack another users account
- Report security problems or misuse to teacher or principal
- Parents/guardians should stay involved in their child's classroom activities, including the use of technology applications
- Adhere to copyright laws and applicable policies and procedures

PK LAW®

Carroll County Public Schools

Improper Use

Students: Improper use of approved technology applications may result in disciplinary action and/or legal action in accordance with federal or state law and CCPS policy. Principal or designee may cancel or limit a student's user privileges or increase supervision of student's use of technology resources, as appropriate.

Staff: Improper use of technology applications or use of non-approved technology applications shall result in disciplinary and/or legal action in accordance with federal or state law and CCPS policy. Investigation of allegations is conducted by Department of Human Resources.

Appeals Process

1. ITRT decision may be appealed to Technology Review Board (TRB), serving as the Superintendent's designee.
    1. TRB composed of Director of Curriculum and Instructional Resources, Director of Technology Services, and Supervisor of Purchasing. TRB may consult with legal representative as needed.
2. TRB decision may be appealed to Board of Education of Carroll County.

PK LAW®

Carroll County Public Schools

What if a teacher wants to use a technology application that has signed the "Student Privacy Pledge"?

The ITRT may forgo its compliance review, but the technology application must still be reviewed according to the ITRT internal procedure for approval of tools (i.e., the tool cannot allow for the secondary use of data for marketing, sales, or targeted advertising, claim intellectual property rights for content uploaded by the user, contain content that is objectionable and/or does not serve an instructional purpose, requires the release of FERPA protected information).

See the Student Privacy Pledge Signatories page: https://studentprivacypledge.org/signatories/

PK||LAW®

Back to the Monday Morning Exercise . . .

- Carroll County Public Schools Policy AF, Administrative Regulation, and Procedure
  - Balance utility of online educational services as a learning tool with protection of student PII
  - Review and approval of tools in accordance with guidelines consistent with Federal and State Law and best practices.
  - Guidelines for use of tools
  - Appeal procedure
  - Consequences for misuse of tools/mishandling student data
- Training of school system staff
- Promote awareness amongst teachers, staff, parents, students
- Review of tools currently in use/proposed for use

PK Law | 901 Dulaney Valley Road, Suite 500 | Towson, MD 21204 | (410) 938-8800 | www.pklaw.com

Adam E. Konstas akonstas@pklaw.com

CASE 1 – ONLY THE TEACHER NEEDS AN ACCOUNT

- A teacher requests an online tool to use to collect videos of students. The tool requires the teacher to create an account and she gives students an access code to join her group. Students then upload short video clips of themselves speaking for the teacher to evaluate.

CASE 1 – ONLY THE TEACHER NEEDS AN ACCOUNT

- Is students' Personally Identifiable Information involved?
- Which provision for disclosure in FERPA would be appropriate to use?

CASE 1 – ONLY THE TEACHER NEEDS AN ACCOUNT

- What types of concerns does this language raise?
- Can this tool be approved?

CASE 2 – HOW MANY SITES ARE INVOLVED?

- NASA is sponsoring a research challenge and hires a privacy company to handle student registration. The company, PRIVO, is primarily focused on COPPA compliance. NASA TOU review checks out and PRIVO looks good. The PRIVO email validation for parent registration indicated that students will be using Glogster.com to create their submission.

CASE 2 – HOW MANY SITES ARE INVOLVED?

- Do the terms for Glogster.com need to be reviewed before the tool can be approved and who is responsible for the data on Glogster – NASA? PRIVO? CCPS?

CASE 2 – HOW MANY SITES ARE INVOLVED?

- Can this contest be approved?
- If the opportunity to participate in the contest is critical, and it cannot be approved, how can we resolve these issues?

CASE 3 – BUT IT'S THE COLLEGE BOARD

- The College Board website provides numerous services to multiple user groups. The College Board is a signatory of the Future of Privacy Forum and The Software & Information Industry Association's "Student Privacy Pledge" indicating that they will protect student data and privacy indicating that they will "not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students." The site is also used by students to register for the SAT and to receive scores from College Board assessments. Many staff members also have accounts.

CASE 3 – BUT IT'S THE COLLEGE BOARD

- If the site were approved, would school system staff be permitted to direct students to create accounts on the College Board site?

CASE 3 – BUT IT'S THE COLLEGE BOARD

- Explain the difference between "behavioral targeting of advertisements" that the College Board has committed to avoid and the "tailored promotions" the TOU is planning to provide?

- Who, if anyone, should be permitted to create College Board accounts in association with their roles in CCPS?

CASE 4 – THIS IS A REQUIREMENT

- Career and Technical Student Organizations (CTSOs) are promoted by MSDE and supported by the Carl D. Perkins Career and Technical Education Improvement Act of 2006. In fact, they are an integral component of the MSDE Career and Technology Education program. Many CTSOs maintain websites aimed at providing information and benefits to members. In most cases, these sites require logins and collection of information about the user.

CASE 4 – THIS IS A REQUIREMENT

- With MSDE oversite and federal support, do sites for these groups need to be reviewed for use?

CASE 4 – THIS IS A REQUIREMENT

- If this site is intended for FBLA advisors and does not permit student to create accounts can it be approved?
- Who is the most appropriate person or role in the school system to clarify the use of and advocacy for content-based tools and sites?

CASE 5 – IT IS JUST A WEBSITE

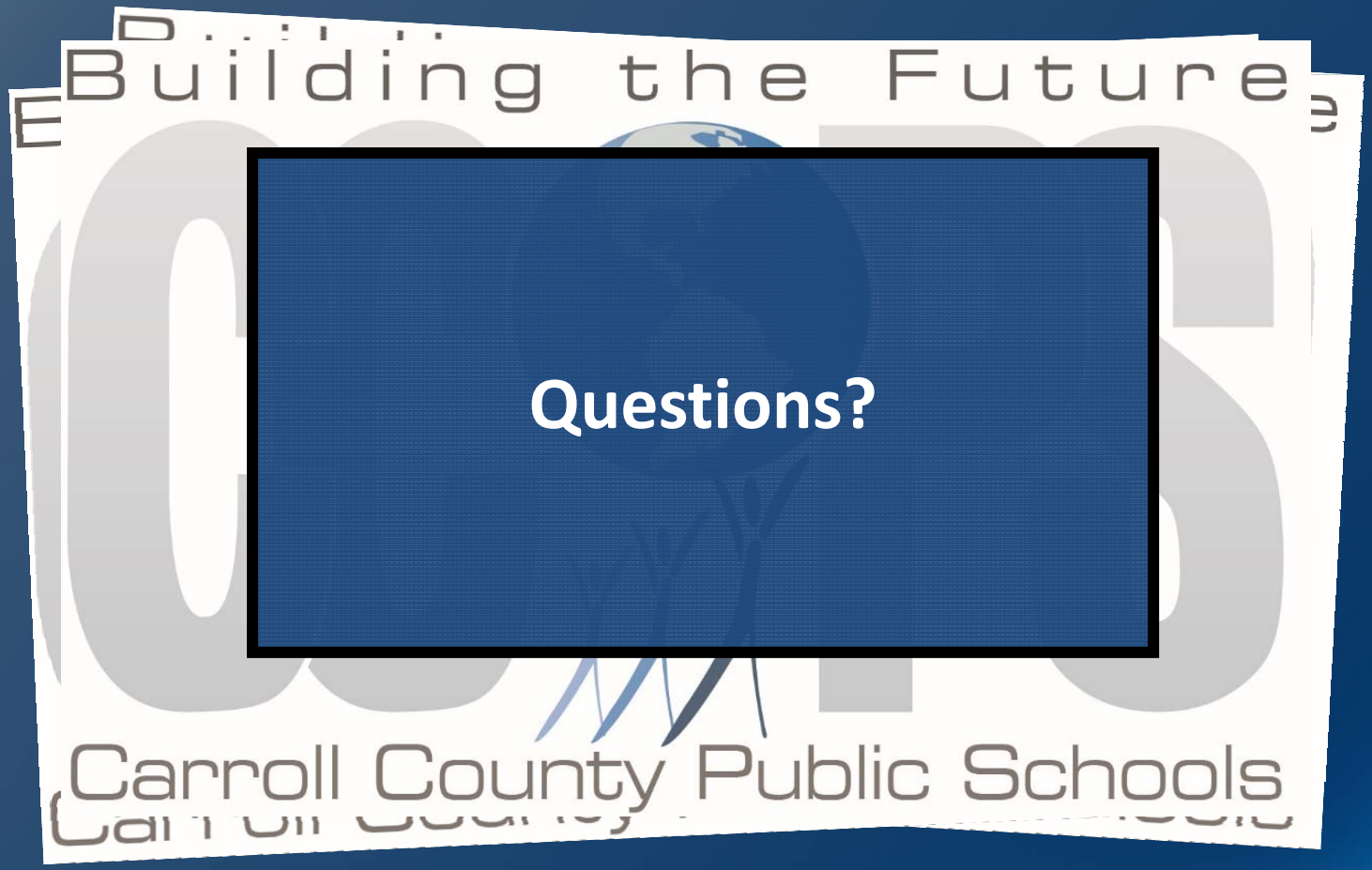
- A teacher requests that a website be unblocked for student use because it is aligned to the curriculum. It is already available to staff logins and the teacher has been able to get valuable information from the site. The workflow for this type of request does not include the ITRT. The instructional supervisor holds the primary responsibility for the approval of the site.

CASE 5 – IT IS JUST A WEBSITE

- What standards should the supervisor use to review the site?

CASE 5 – IT IS JUST A WEBSITE

- Should this website be reviewed and approved following the Student Data Privacy procedures?



Questions?