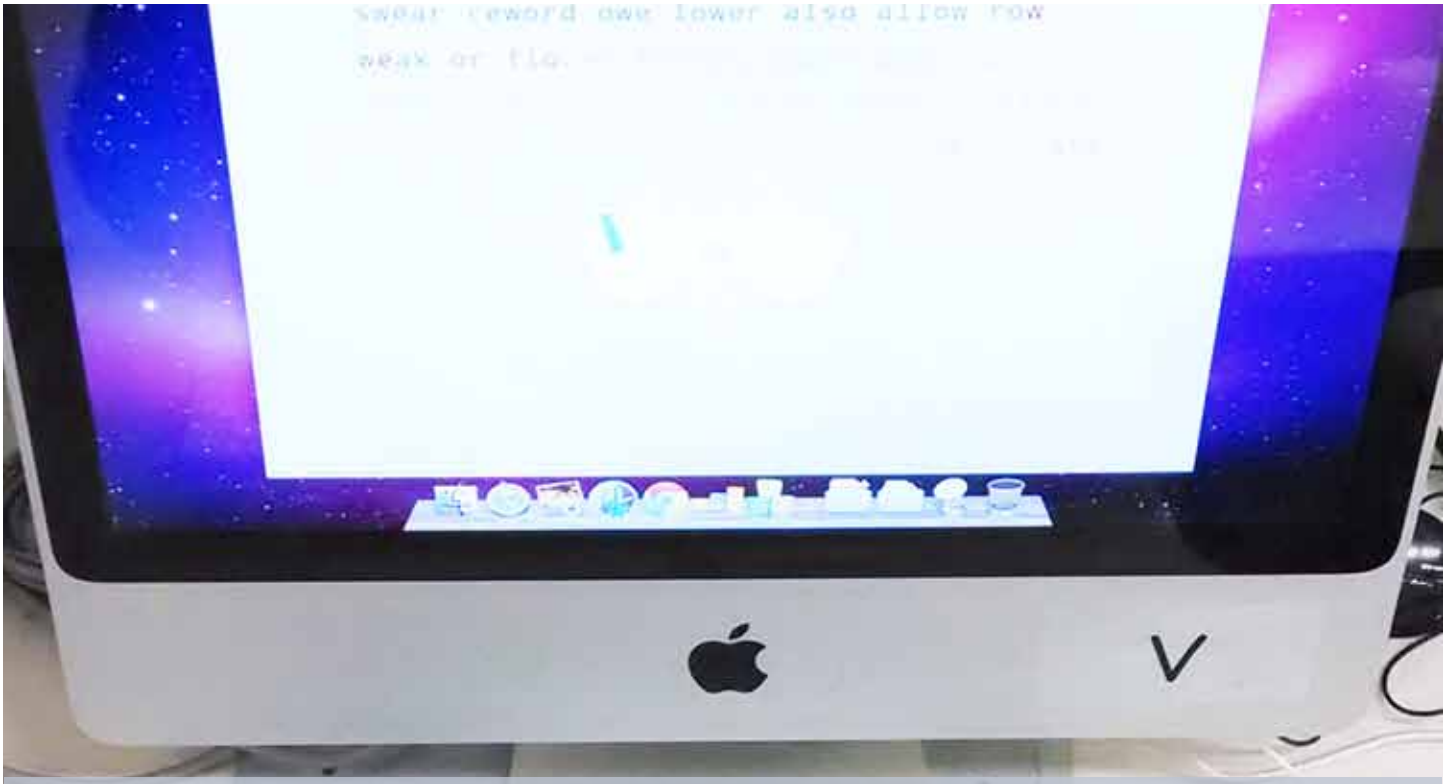


Balancing Classroom Innovation & Student Privacy

CPS
Cambridge Public Schools

Contents

Balancing Classroom Innovation & Student Privacy

WWW.CPSD.US

Executive Summary

Cambridge Public Schools (CPS) are rich with technology resources and capacity to support innovative teaching strategies. As a leader in this area, CPS is at the forefront of balancing student privacy within current laws, while encouraging innovative uses of technology at the classroom level.

In today's world of advancing on line resources teachers, students and parents are benefiting from an ever increasing wealth of tools to support teaching and learning. These new tools are enabling data rich applications that are available anytime anywhere creating an online learning environment that technology proponents have promised for years. The growth in these tools is extraordinary with great potential to improve student outcomes.

Along with this explosion in growth of online learning tools, comes the inherent risks of leakage of student data and understandable concerns over student privacy. This video (associated to the Trust Challenge - a grant opportunity focused on building trusted learning environments) provides some clarity around the issue through various perspectives; teacher, student, parent, technologist, out of school time provider. In many ways, CPS is also attempting to create "21st Century Systems of Trust" within the district, and the city as a whole, to best serve our students, while ensuring their privacy online.

In an attempt to support innovation and the leveraging of these new tools to support teaching and learning CPS has developed internal processes to vet and adopt secure online systems. This process is sometimes seen as a barrier to the adoption of great new tools. Balancing the adoption of new tools with the obligation to protect student privacy while being agile and supportive of classroom innovation is the challenge.

This document intends to outline the "challenge" by discussing each contributing factor including; Laws governing student privacy, CPS data systems, online or "Cloud" services, and the current CPS "Digital Resources Procedure". This document should be considered a starting point for discussions with some recommendations for next steps.

CPS
Cambridge Public Schools

VISION STATEMENT

The Information, Communication, and Technology Services (ICTS) department is a collaboration among Library Media, Educational Technology, Media Arts, Web Services and Technical Services divisions. This department strives to support administration and teachers; inform parents; and to prepare students for lifelong learning, informed decision-making, a love of reading, and the use of information and communication technologies.

ICTS LEADERSHIP TEAM

Steve Smith
Chief Information Officer

Marjorie Berger
Assistant Director of Library Media Services

Ginny Berkowitz
Media Arts Manager

Kevin Keegan
Technical Services Manager

Gina Roughton
Assistant Director of Educational Technology

Lisa Waters
Web & Online Services Manager

459 Broadway
Cambridge, MA 02138
617.349.9360
Fax: 617.349.6800
www.cpsd.us

Laws

Family Educational Rights and Privacy Act (FERPA)
Protection of Pupil Rights Amendment (PPRA)
Children's Online Privacy Protection Act (COPPA)
Children's Internet Protection Act (CIPA)
Massachusetts Student Records
Massachusetts Data Breach Law
Massachusetts Data Destruction Law
CPS Policies

Family Educational Rights and Privacy Act (FERPA)
20 U.S.C. §1232g and 34 C.F.R. 99.1-99.35

This federal law and its related regulations prohibit school districts from disclosing, except in certain limited instances, personally identifiable information that is contained in a student's educational record without the consent of the parent/guardian or the student. An educational record includes any written or electronic files, including emails and other communications or materials that are created by the student, teacher or school administrator that (i) contain information directly related to the student, and (ii) are maintained by the educational agency or institution or by a person acting for such educational agency or institution. School districts are required to notify students and their parents/guardians on an annual basis of their rights under FERPA. Currently, the school district has taken the prudent approach of presuming that all data related to students is an "educational record" and seeks to retain control over that data.

Protection of Pupil Rights Amendment (PPRA)
20 U.S.C. §1232h and 34 C.F.R. Part 98

This federal law and its related regulations require school districts to make certain instructional materials available for inspection by parents/guardians and to obtain consent from parents/guardians of students who are scheduled to participate in activities involving the collection, disclosure or use of personal information from students for marketing purposes, to to obtain consent from parents/guardians of students before selling or otherwise providing personal information of students to others for marketing purposes and to give parents/guardians the opportunity to opt-out of these activities. Protected personal information includes: (i) political affiliations or beliefs of the student or the student's parents/guardians; (ii) mental or psychological problems of the student or the student's family; (iii) sex behavior or attitudes; (iv) illegal, anti-social, self-incriminating or demeaning behavior, (v) critical appraisals of other individuals with whom respondents have close family relationships; (vi) legally recognized privileged or analogous relationships, such as those of lawyers, physicians and ministers; (vii) religious practices, affiliations or beliefs of the student or the student's parents/guardians; and (viii) income other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program. School districts also are required under this law to develop policies in consultation with parents/guardians on the collection, disclosure and use of personal information collected from students for the purpose of marketing or selling

that information. School districts also are required to provide annual notice of its PPRA policies to parents/guardians, provide parents/guardians with an opportunity to opt their child out of any instructional activities related to these subjects, and to provide notice to parents/guardians when there will be specific activities occurring around any of these subjects. An interplay can occur between FERPA and PPRA when a school district provides FERPA protected data for the purpose of opening a student online account for an educational service and then subsequent information that is gathered through the student's interaction with the online account implicates the provisions of PPRA.

Children's Online Privacy Protection Act (COPPA)
47 U.S.C. §231

This federal law is specifically designed to protect the privacy rights of children under the age of thirteen (13). The law requires that commercial websites and online services that are directed at children obtain parent/guardian consent before the collection or use of any personal information regarding a child. Personal information includes: (i) child's first and last names, (ii) home address, (iii) email address, (iv) telephone number, (v) any identifier that if used over time could be used to identify a user across different websites, (vi) any photograph, video or audio file that contains a child's image or voice, (vii) geo-location information that can provide a street or town name, and (viii) information that a commercial website or online service can collect online that would concern either the child or the child's parents/guardians and then combine with any of the identifiers listed above. School districts contracting with commercial websites and online services need to examine the operator data collection, use and sharing policies before agreeing to act as an agent or intermediary for parents/guardians in terms of granting consent for a student to go on line and utilize the services of a commercial website and/or online service. If a school district is going to provide consent for students for the collection of student personally identifiable information, it must notify the parents/guardians in advance of doing so. This is typically done through the use of a consent form seeking the parents/guardians consent for such information to be provided through or to a commercial website or online service. COPPA does not apply if the school district is contracting directly with the website or online service for the sole benefit of the school's use of its student data. Additionally, COPPA requires that the commercial website or online provider obtain consent from the parents/guardians of a student when it intends to use or disclose a child's personal information for its own commercial purposes in addition to the provision of services for the sole benefit of the school. An interplay can occur between FERPA and COPPA when a school district provides FERPA or COPPA protected data for the purpose of opening a student online account for an educational service and then subsequent information that is gathered through the student's interaction with the online account implicates the provisions of COPPA.

Children's Internet Protection Act (CIPA)
20 U.S.C. §§6801, 6777, 9134; 47 U.S.C. §254

This federal law is designed to protect children from access to obscene or harmful content over the Internet by imposing certain requirements upon schools and libraries that receive discounts for the Internet and internal connections through the federal E-rate program. More specifically, school districts must have an Internet safety policy that includes technology protection measures to block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors. Additionally, the Internet safety policy must address: (a) monitoring online activities of minors, (b) access by minors to inappropriate matter on the Internet: (c) safety and security of minors when using electronic mail, chat rooms or other forms of direct electronic communication, (d) 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, (e) unauthorized access, including "hacking" and other

unlawful activities by minors online; (f) unauthorized disclosure, use and dissemination of personal information regarding minors; and (g) measures designed to restrict minors from accessing material that is harmful to minors. Issues related to compliance with the requirements of CIPA arise when schools are utilizing online activities with students.

Massachusetts Student Records
M.G.L.c. 71, §§34D & 34E and 603 C.M.R. 23.00 et seq.

This state law and related regulations, like its federal counterpart FERPA, is designed to protect parent/guardian and student rights regarding the confidentiality, inspection, amendment and destruction of student records. A student record consists of the transcript and temporary record, including all information, recordings and computer tapes, microfilm, microfiche, or other materials, regardless of physical form or characteristics, that is kept by a school district concerning a student that is organized on the basis of a student's name or in a way that such student may be individually identified. School districts are required to notify students and their parents/guardians on an annual basis about their rights under the student records laws and regulations.

Massachusetts Data Breach Law
M.G.L.c. 93H

This state law requires any business entity or person that owns, licenses, maintains or stores "personal information" to have measures in place to prevent disclosure of personal information and notify affected individuals if there has been a data breach. Personal information is a person's first and last name or first initial and last name in combination with either: (i) social security number, (ii) driver's license or other state issued identification card number or (iii) a financial, account number, credit or debit card number with or without any required security code, access code or PIN. The Massachusetts data breach law can be implicated if an online provider is maintaining personal information regarding a student including the student's first and last name or first initial and last name in combination with either a social security number or state issued identification number.

Massachusetts Data Destruction Law
M.G.L.c. 93I

This state law utilizes the same definition for personal information as the state's data breach law along with the additional element of biometric indicators. This law requires that paper documents containing personal information be redacted, burned, pulverized or shredded and that electronic media and other non-paper media containing personal information be destroyed or erased so that personal information cannot be read or reconstructed. Third parties who are handling the disposal of such personal information must have procedures in place to prevent unauthorized access to the information. The law also provides for the imposition of fines for improper destruction. This law can be implicated is an online provider is maintaining personal information regarding a student and the information is to be destroyed.

Pending Legislation

The area of student privacy and its relationship to technology continues to evolve. There is currently legislation pending at both the federal and state level to add additional protections to protect student personal information that is maintained by cloud providers that provide educational services, including restricting the ability of these providers to use such information for marketing and advertising purposes. The school district continues to monitor changes in the law and make necessary adjustments to its practices and procedures to comply with any new laws and regulations as promulgated.

Challenges Presented by "Click-Wrap" Terms of Use

The "click wrap" terms of use and privacy policies that are established by cloud service providers typically are posted on the bottom of the web page for the provider. These are the non-negotiable terms to which a user agrees when utilizing the cloud service providers products or services. Among the variety of provisions that can present a challenge in these agreements are the following types of provisions:

(i) Choice of Law/Choice of Forum Provisions

A choice of law clause describes what state or country's laws will decide the outcome of a dispute between a user and the cloud service provider. If parties get involved in a legal dispute, then the dispute will be decided by the law of the place chosen by the choice of law provision. The choice of law governing an agreement is relevant because laws can vary between states and/or countries. A choice of forum clause decides where a dispute will be physically filed and tried. This provision can establish a different state or a different country from where the user is located as the forum for resolution of a dispute between the parties.

(ii) Indemnification Provisions

Indemnification clauses shift costs between parties when certain conditions (as detailed in the clause) occur. These provisions, when agreed to, can for make the user responsible to legally defend a cloud service provider, hold a cloud service provider harmless, or pay a cloud service provider's legal costs.

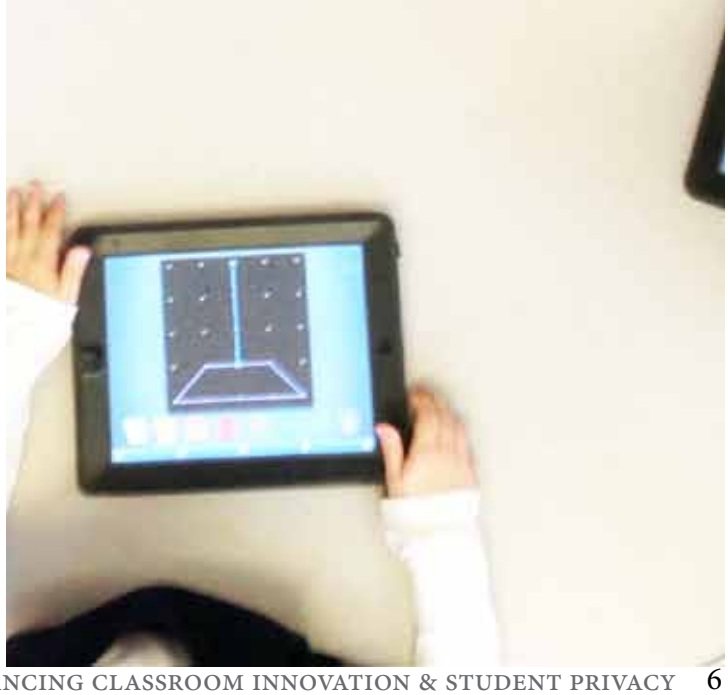
(iii) Use and Maintenance of User Data

Cloud service providers often include clauses in their "click wrap" agreements that indicate when, how and to what extent the provider has control over a user's data. Such provisions can include, but not be limited to, provisions dealing with control and access to data by the cloud service provider and/or other third parties associated with the cloud service provider, the ability of the cloud service provider to utilize (or not utilize) the data for marketing/advertising, and how data will be maintained and/or destroyed by the cloud service provider when no longer needed.

CPS Policies

Attached to this document as appendixes are the following related policies:

- Acceptable Use Policy
- Software Code of Ethics Policy
- School and District Web Pages Policy
- Website Privacy Policy
- Student Records Policy
- Student Privacy Policy
- Student Record Administrative Guidelines
- Technology Use Administrative Guidelines

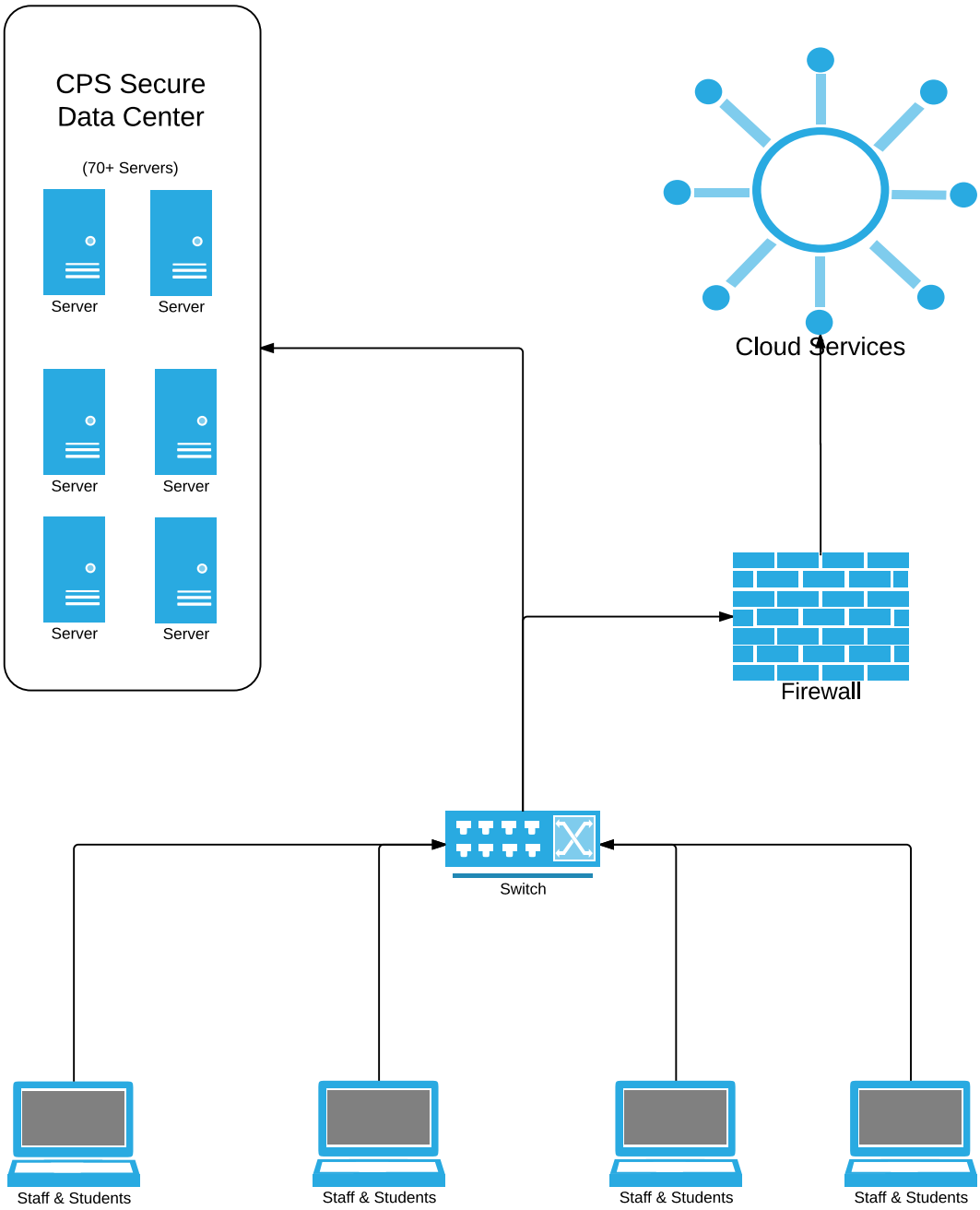


CPS Data Systems

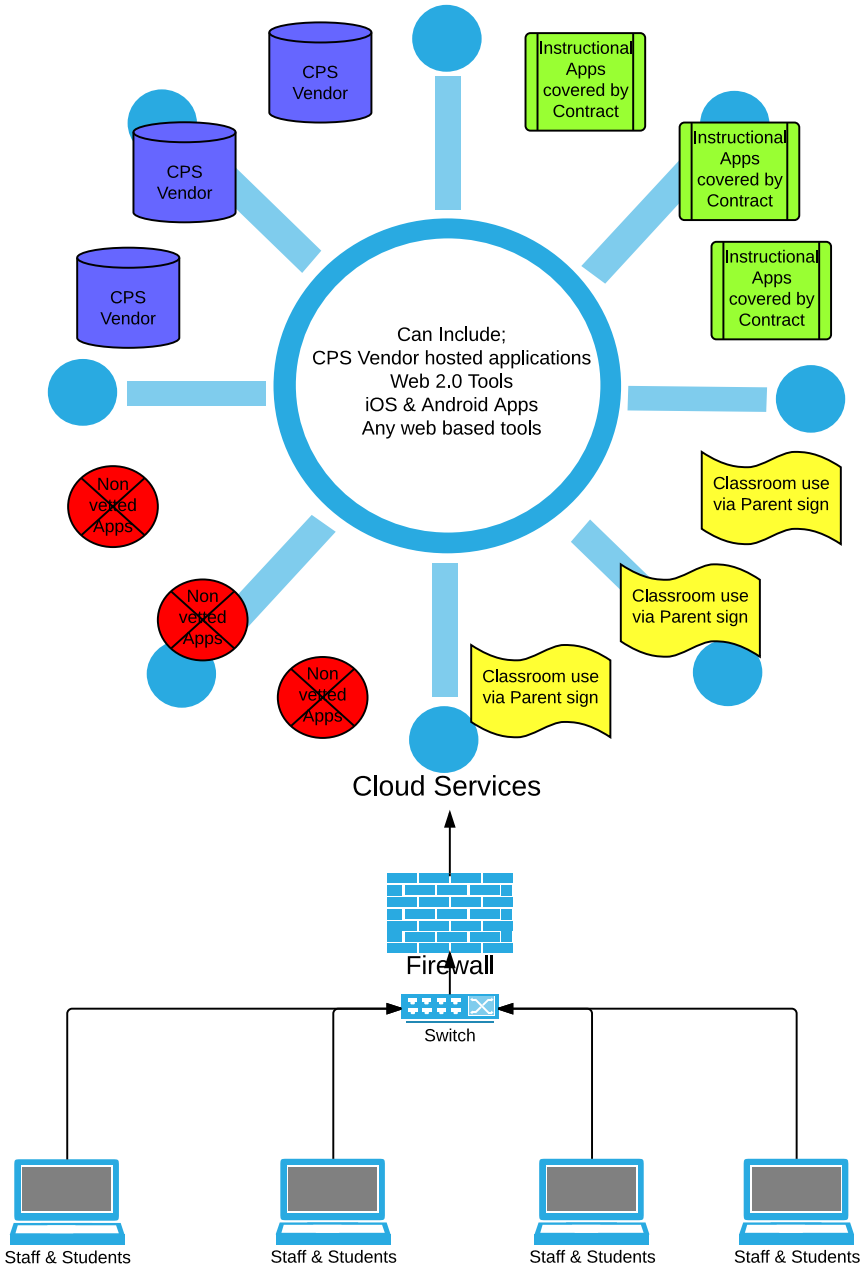
CPS Core data systems are maintained on servers that are physically located within a secure data center at CRLS.

These servers are owned, controlled and monitored by CPS. All access is controlled and logged. There are 70 plus servers, most of which have been virtualized, located within the CPS data center.

Since CPS has physical possession of these servers and CPS controls the security and access we can ensure that student privacy is 100% protected in accordance with the applicable laws.



Online "Cloud" Services



"Cloud" services have many interpretations. For this demonstration, "cloud" will mean any service not hosted within CPS data center.

Cloud based services utilized by CPS can be divided into four categories; CPS Vendor hosted solutions, Instructional applications for which CPS has a student data contract, classroom applications for which parental authorization is obtained per student, and other applications for which there is no contract or parental sign off.

When any CPS staff engage our students with an online application that in any way captures student level data, whether personally identifiable information or simply student generated content, CPS has an obligation to ensure that the data is protected regardless of where the data is housed.

Three of the four scenarios described adequately protect the privacy of our students. The red non-vetted apps expose potential student privacy issues.


lenovo

Digital Resource Procedures

CPS Digital Resource procedures were developed as a mechanism to ensure all student online activity is properly vetted and student privacy is protected.

The procedure mirrors recent guidance from the US DOE Privacy and Technical Assistance Center published in their document "Protecting Student Privacy while Using Online Educational Services". These guidelines were based partially on findings included in the Berkman Center's Student Privacy Initiative's publication entitled "*Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014*".

As departments, schools, and teachers identify resources to support teaching and learning, they are supported in evaluating the level of student data that is shared through the application and taking the appropriate steps to ensure security of the data. Departments and schools typically connect with the ICTS department during the search phase for a resource and through a collaborative effort the appropriate digital resource is selected and a Student Data Data Breach Agreement is executed. Teachers have an ICTS school-based team with which they can initially consult regarding available and appropriate resources, if a new resource is identified, there is a Digital Resources Request Form to submit which asks detailed information about the resource, intended use, and instructional purpose. The submitted form is then reviewed by the ICTS department to identify alignment with instructional purpose, overlap with existing resources, and to pursue a Student Data Data Breach Agreement with the company. If the company refuses to sign the Student Data Data Breach Agreement, the ICTS department then consults with CPS Legal Counsel to draft a parent release for the teacher to use the resource. On occasion, CPS Legal Counsel may advise that a parent release not be drafted given concerns in the language of the company's Terms of Service or Privacy Policy documents. In this case, the request and information is forwarded to the Assistant Superintendent of Curriculum, Instruction and Assessment to determine if the district elects to adhere to the advice of Legal Counsel or pursue use of the ressource.

The Digital Resource procedure has been in place for 3 years and over that time we have secured 55 signed Data Breaches, had 29 companies decline to sign the Data Breach, and drafted 19 parent releases (see attached spreadsheet of Digital Resources contracts). Signed Data Breaches range from resources that support department initiatives such as Houghton Mifflin - Math in Focus (Math) and Impact Applications (Athletics), resources that support school initiatives such as Reading Assistant (Haggerty) and Achieve 3000 (PAUS & VLUS), to applications that are identified by the Educational Technology department in supporting 21st century learning such as Glogster (multimedia digital posters) and Voicethread (sharing and commenting online).

Digital Resource Case Studies

Voicethread
Houghton Mifflin Harcourt: Math in Focus
Teaching Strategies GOLD
Khan Academy
Scratch
Turnitin

Voicethread

Voicethread is an online application that allows users to communicate, collaborate, create, connect, and comment in the cloud. Teachers and students can post content and have a conversation through visuals and a variety of comment media. Students can share their work and reflect, peer review, or collaboratively present. Voicethread hosts a separate educational environment that allows teachers to create class structures and manage student accounts and content. Furthermore, Voicethread integrates with Google Apps for Education to allow single sign on through student Google accounts, which provides a seamless connection to minimize loss of instructional time. Voicethread readily signed the CPS Student Data Data Breach Agreement and we have recently purchased a K-12 license to offer this tool to all schools, teachers, and students.

Houghton Mifflin Harcourt

Math in Focus was recently selected and implemented as the core resource for the math curriculum in grades K-8. Along with this resource comes the feature of student accounts to access online virtual manipulatives, online student interactivities, and a Bar Models iPad app for the lower grades. Houghton Mifflin Harcourt signed the CPS Student Data Data Breach Agreement and we are currently distributing student accounts to teachers and math coaches to support the use of these online resources.

Teaching Strategies GOLD

Teaching Strategies GOLD is the online tool CPS has selected to implement the Massachusetts Kindergarten Entry Assessment (MKEA). It is an evidence-based assessment system that provides a teacher account structure for inputting and managing the collection of evidence across a series of domains. This school year is the first year of implementation and kindergarten teachers are collecting evidence in the Social/Emotional domain. Evidence includes photos, notes, and images of student work. Teaching Strategies GOLD signed the CPS Student Data Data Breach Agreement. Additionally, as photos and other images of students are collected and uploaded, parents/guardians are asked to sign the school district's general media release or, in the alternative, a specific media release for the sole educational purpose of the Teaching Strategies GOLD MKEA assessment.

Khan Academy

Khan Academy is an educational organization with a mission of "providing a free world-class education for anyone anywhere." Students can freely access content through sample problems, video lectures, and challenges. Teachers/coaches can set up accounts to support students through this work and guide their path. Teachers in CPS identified this as a potential resource for differentiating instruction in the classroom and requested to use it with student and teacher accounts. Khan Academy declined signing the CPS Student Data Data Breach Agreement citing "we do not enter additional legal contracts at the school/district level for the usage of our site, but rather abide by the policy we set in our privacy policy." The CPS legal department subsequently drafted a parent/guardian release that teachers could distribute with a copy of the Khan Academy Terms of Service and Privacy Policy to parents for signature and use with students.

Scratch

Scratch is a programming tool developed by the Lifelong Kindergarten Group at the MIT Media Lab that allows users to "think creatively, reason systematically, and work collaboratively" in a programming language environment. The open-ended nature of the tool allows for many applications within the curriculum and learning in CPS. Teachers expressed interested in students not only using the downloaded software, but also creating online accounts to share, collaborate and remix projects to expand their learning and foster 21st century skills. The developers of Scratch were unable to sign the CPS Student Data Data Breach Agreement due to the nature of the research group. The CPS legal department subsequently drafted a parent/guardian release that teachers could distribute with a copy of the Scratch Terms of Service and Privacy Policy to parents for signature and use with students.

Turnitin

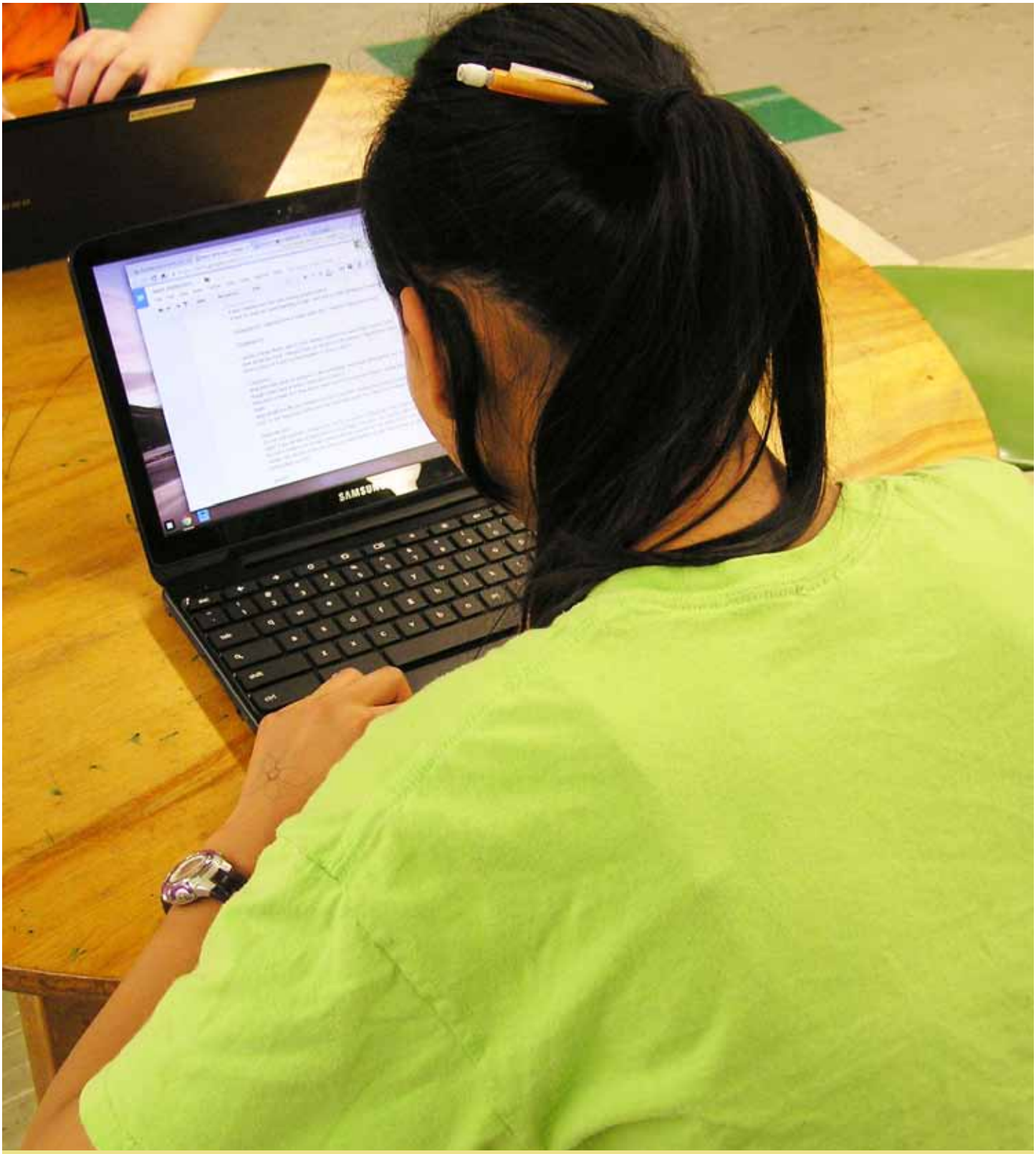
Turnitin is a cloud-based service for originality checking that was in use by CRLS faculty as the Digital Resources procedures were initially implemented. Teachers and students within the ELA department were using the service to submit writing and receive feedback. With the implementation of the Digital Resources procedures, a request was made to Turnitin to sign the CPS Student Data Data Breach Agreement. Turnitin declined signing the Student Data Data Breach Agreement. The CPS Legal Department was able to draft a parent/guardian release for teachers could distribute along with a copy of Turnitin's Terms of Service and Privacy Policy to continue use of the service, including highlighting Turnitin's retention of student work as part of its database for future use in connection with its plagiarism-prevention services. Upon distribution of the parent/guardian release, some parents/guardians raised concerns Turnitin's retention and use of student work as stipulated in its Terms of Service. These concerns resulted in those parents/guardians refusing to sign the release and thus posed a challenge for the teachers to utilize the service with all of their students. Ultimately, CRLS administration made the decision to stop use of the product for these concerns as well as the pricing structure of the product and its limited use within the school.

Summary

Today's learning environments are no longer confined to within the school walls. A great deal of learning activity occurs in a rapidly growing online environment of new and innovative learning tools. We have an obligation to ensure that all students' privacy is protected when operating in these complex online applications. There are many laws governing CPS's obligation to protect privacy as well as local policies and procedures to ensure adherence.

The local CPS procedures are an ever changing set of guidelines meant to ensure student privacy in a rapidly changing world on online tools and laws. Moving forward some items to consider may include;

- Continued refinement of CPS Digital Resource procedures
- Identification of CPS Student Privacy Officer or role
- Clearer guidelines around data terms of service that are acceptable and not acceptable
- Increased education with staff, students, parents/guardians and community around student privacy issues
- Greater transparency of data sharing practices, including data elements shared and contractual language with vendors
- Continued work towards greater acceptance of standard student data privacy norms & practices through partnerships with the Harvard Law School Berkman Center Work and other local districts



www.cpsd.us