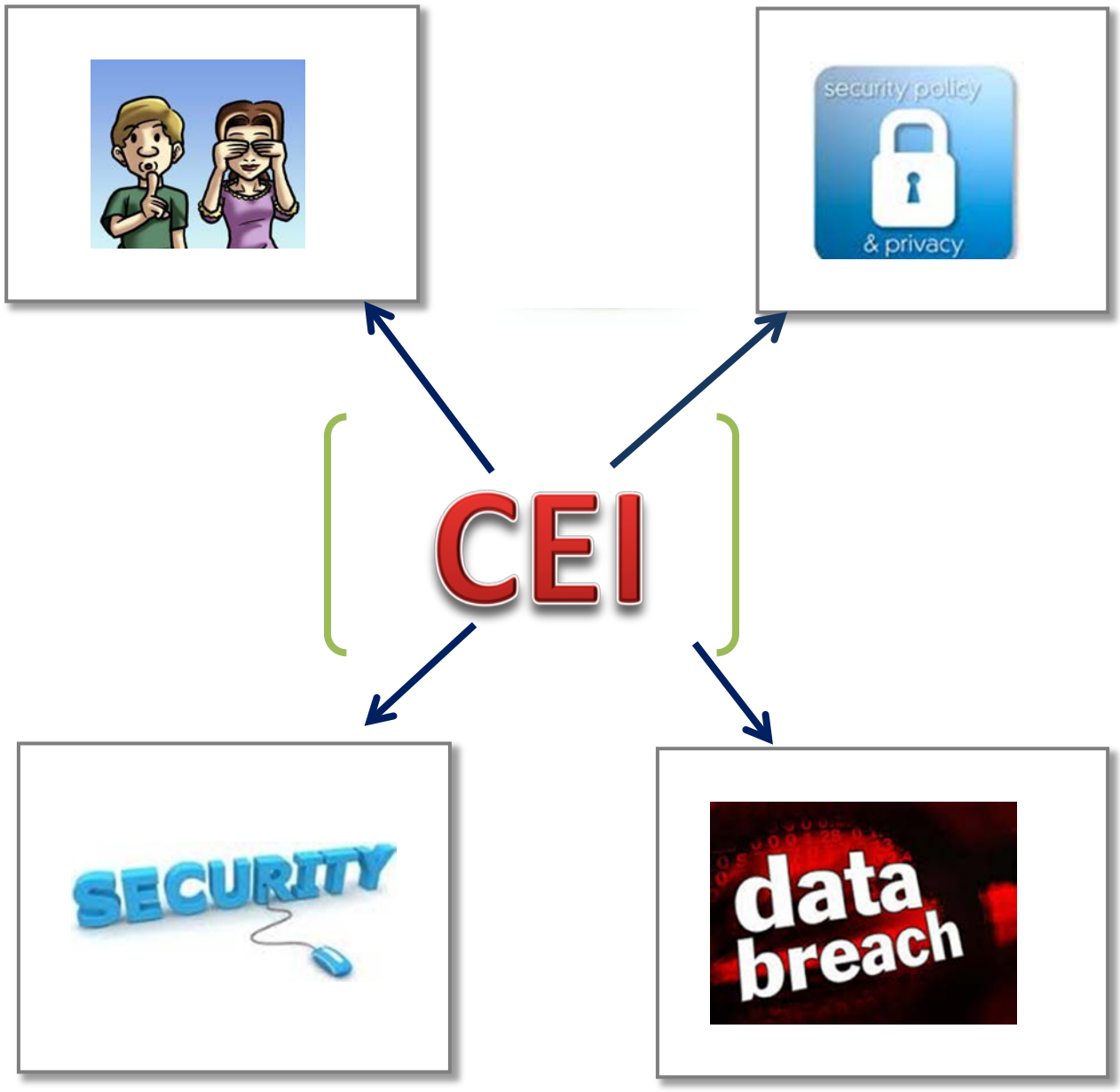


CENTER FOR EDUCATIONAL INNOVATION

Privacy and Security Policy

First Edition

CENTER FOR EDUCATIONAL INNOVATION

Board of Trustees

Judy Roth Berkowitz	Chairperson
Seymour Fliegel	President
Donald Cecil	Treasurer
Dean Ringel, Esq.	Secretary

Norman S. Benzaquen
Anthony Paul Coles, Esq.
Mary Ellen Fahs, Ph. D.
Sherry R. Jacobs, Esq.
Marian Klein
Clay McDaniel
Robert Sancho
Ann Rubenstein Tisch
Nathan Glazer, Honorary Member
Steve B. Klinsky, Honorary Member

CEI-PEA Standards Operating Procedures (SOPM)
TABLE OF CONTENTS

WELCOMING MESSAGE FROM THE PRESIDENT/CHIEF EXECUTIVE OFFICER

CEI recognizes the importance of protecting the privacy and confidentiality of certain information collected by our staff as we strive to improve teaching and learning in K-12 schools. Towards this goal, CEI has established this privacy and security policy to summarize how we collect, use, share, store and protect information that we may gather on or off-line from the New York City Department of Education and New York/New Jersey Charter Schools. This policy does not apply to information that we may collect, such as over the phone, by fax, or through conventional mail. All educational records are protected by CEI as required by the federal Family Educational Rights and Privacy Act and similar state laws. CEI may amend this policy from time to time and will prominently display on our Web site any substantial change in the way we use sensitive information. Such information is available at www.thecei-pea.org.

Seymour Fliegel
President/Chief Executive Officer

CEI PRIVACY/SECURITY POLICY

What is the purpose of this policy?

CEI is committed to the highest level of integrity as we strive to enable data driven instruction and accountability at the school level. This policy is designed to assist you in understanding how digital information entrusted to CEI is secure, to ensure you that all applicable regulations regarding privacy and security of data are followed, and that informed decisions are made when educational communities use our web sites, curricula and services. This statement will be continuously assessed against new technologies and educational business practices.

This digital information security policy calls for the utilization of appropriate safeguards to protect sensitive and/or protected information resources based upon the sensitivity of the data in question, legal requirements, and risks to CEI. It explains what can be expected with regard to digital data resources classification, responsibilities for developing appropriate security measures, and guidelines for securing electronic systems.

Although we take appropriate measures to safeguard against unauthorized disclosures of information, we cannot assure that personally identifiable information that we collect will never be disclosed in a manner that is inconsistent with this Privacy/Security Policy.

An exhaustive discussion of the details of CEI's security infrastructure would be inappropriate for a published document for security reasons. However, all appropriate means to protect the data we collect and handle are in place including, but not limited to:

- Encryption of data in transit via Simple File Transfer Protocol, Virtual Private Network access
- Review and testing of application code for security issues
- Firewalls
- Access management for systems used by DOE employees and/or partner agencies
- Web blocking and monitoring implementation
- Patch management of all servers and end user workstations

- Backup and offsite secure storage
- Asset management.

What information do we collect/store?

When you use our websites (http://www.thecei-pea.org and https://www.mypiccs.org) to read pages or download information, we will automatically gather and store certain information about your visit. We use this information to help us make our site more useful to visitors to learn about the number of visitors to our site, and the types of technology our visitors use. We do not give, sell, or transfer any of this information to a third party. As a not for profit organization working with schools, we are subject to the access and confidentiality provisions of the applicable laws, and we will therefore disclose personally identifiable information as required by law, for example, in response to a court order, a subpoena, or a law enforcement or regulatory agency's request.

Only the following information about your visit is automatically collected and stored:

- The Internet domain (such as "youragency.gov," "yourschool.edu," or "yourname.com") and IP address (the number that is automatically assigned to your computer whenever you are browsing the web) from which you access our site
- The type of browser and operating system used to access our site
- The date and time you access our site
- The pages you visit, and, if you linked to our site from another site, the address of that site.

The logs may be preserved indefinitely, and they may be used to prevent security breaches and to ensure the integrity of the data on our servers.

Email addresses obtained through CEI's websites or headquarters will not be sold or given to other private companies for marketing purposes. The information collected is subject to the access and confidentiality provisions of the Public Records Act, other applicable sections of the New York State code as well as federal laws. Email or other information requests sent to the CEI's websites may be retained in order to respond to the request, may be forwarded to the appropriate staff at CEI, may result in updates to CEI's web pages that may be of interest to citizens, or may provide CEI's websites designer with valuable customer feedback to assist in improving the site. Individuals can cancel any communications regarding new service updates at any time.

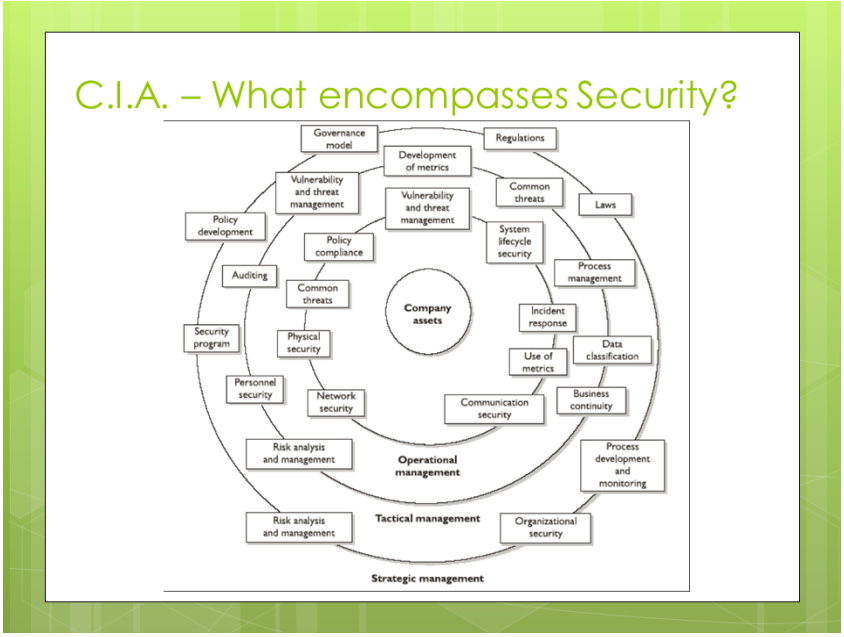
How do we use data provided to us?

Broadly speaking, we use personal data provided to us for purposes of teacher/student improvement. The Partnership for Innovation in Compensation for Charter Schools (PICCS) is a human capital management system (HCMS) that is in various stages of implementation at 31 public charter schools in New York and New Jersey. Developed through a series of federal Teacher Incentive Fund (TIF) grants, PICCS helps schools support educators and school leaders to become highly effective professionals capable of delivering customized educational programs that result in continuous student growth. CEI analyzes the data gathered to increase compensation paid to teachers in the program. (http://www.mypiccs.org/)

What are cookies?

A cookie is a temporary code placed in your computer by our server that facilitates communication. Our site uses cookies to speed navigation, keep track of the type of services requested, provide you with custom-tailored content and help us determine whether you came to our site from a particular Internet link or banner advertisement. We also use cookies to remember information you previously gave us so you don't have to reenter it each time you visit the site. We do not and cannot use cookies to retrieve personal information about you from your computer unless such information was knowingly and willingly provided by you. You can adjust the settings on your computer to decline any cookies if you wish. This can be easily done by activating the "reject cookies" setting in your browser. However, doing so may slow the response time when you visit our site.

CEI Technology staff monitors HQ servers/computers frequently to ensure proper usage and to avoid vulnerability.

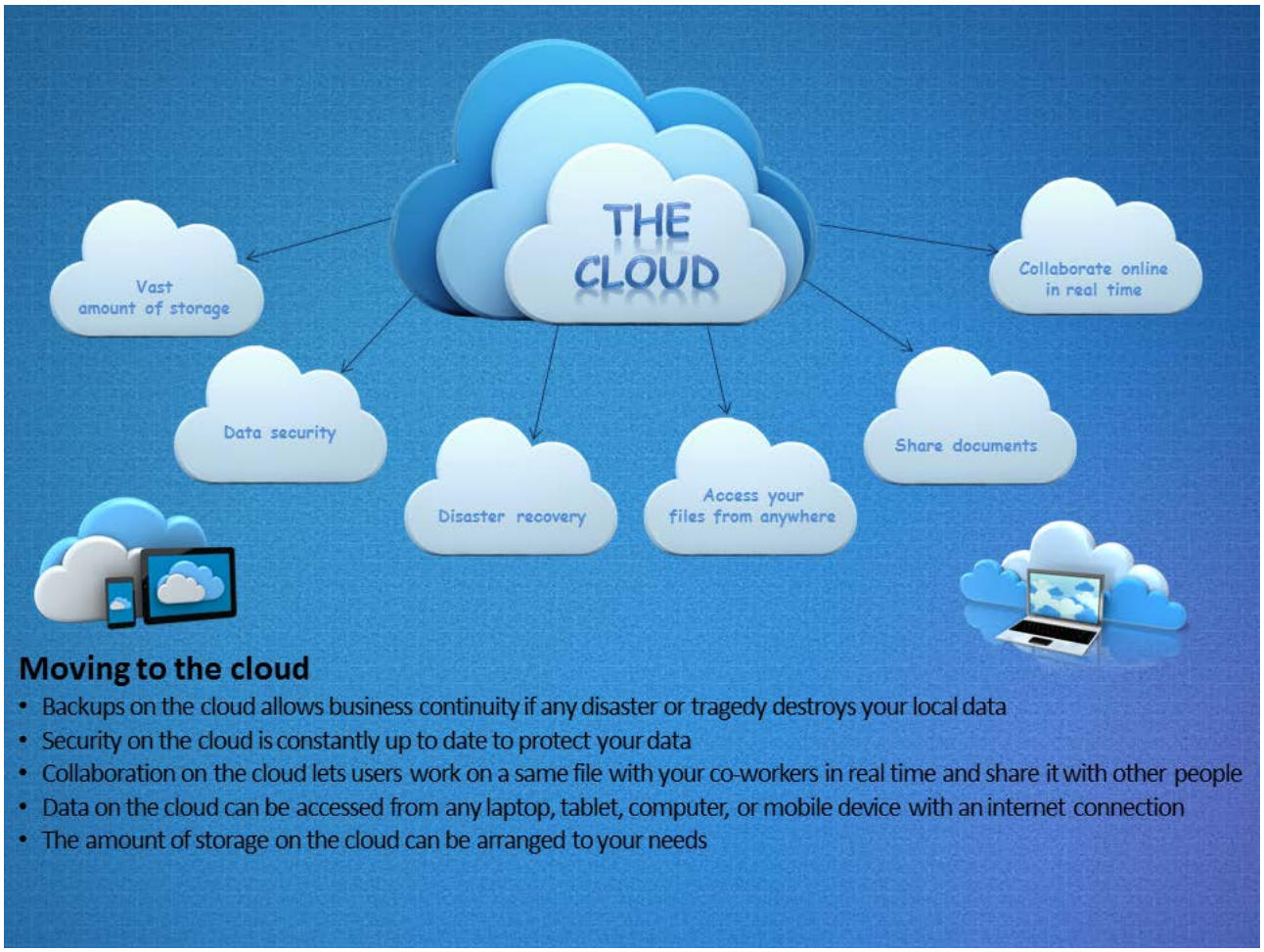


How are our computers/devices/networks secured?

CEI utilizes many technologies to ensure data and network security. Among these are:

- **Unified Threat Management (UTM) Device** technology which includes firewalls with multiple layers of defense against digital attacks and protection of internal data from hackers. It allows for better security when transmitting student data using SSL ("Secure Sockets Layer," protocols designed to provide communication security over the Internet) and blocks threats over commonly used communication protocols such as email, instant messaging (IM), peer-to-peer (P2P), file sharing, games, etc. It includes filtering of web content, and provides static IP addresses for network equipment, servers and workstations.
- **Managed Switches** which are used for creating or modifying VLANs (Virtual Local Area Networks) to segregate traffic and data, and providing physical port restrictions to block unknown devices.
- **Wi-Fi Access Point (AP) Controller** Technology which provides strong encryption using the WPA2 protocol (to secure wireless computer networks), unique SSID (service set identifier) for private and guest networks, and authentication of devices wishing to connect to a network using the 802.1x protocol.

- **Server Security** which limits access to unauthorized personnel. All CEI servers are locked in physical locations, and require complex passwords for access. They are regularly and fully patched with the latest updates, including antivirus protection. They include UPS (uninterruptible power supply) protection against power outages, are accessible only through assigned local groups membership and permissions, and include remote access for administration purposes. The CEI file share servers require strict permissions to access their data; various levels of access can be assigned, such as groups with "read-only" or "full control" access.
- **Cloud-based backup system which utilizes the virtualization of local servers**.



- **Single domain** which ensures all CEI workstations are on the CEI domain; CEI staff use strong passwords, some have encrypted hard drives. As with the servers, they are fully patched and antivirus protected. Local software provides firewall and intrusion prevention. Remote access is enabled, and each workstation is constantly backed up.
- **Anti-virus/spam/phishing protection** which provides the CEI email system with both inbound and outbound filtering.
- **Internet access** which includes filter lists to protect against certain website threats, malware scanning**,** bandwidth restrictions**,** and port blocking on outbound traffic and internet monitoring.
- **Usage logs** from all equipment which are kept on a local server.

What data risks are present regarding CEI networks?

CEI recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access to confidential information within agency records by employees or others
- Unauthorized requests for access to agency records
- Interception of data during transmission
- Loss of data in a disaster
- Corruption of data or systems
- Misplacement or loss of paper records
- Compromise of data from disposal of records
- Unauthorized or unintended disclosure of digital or printed.

What responsibilities regarding data and communications are expected of contracted vendors?

CEI requires contracted vendors working with teacher/student data to:

- Use a "Host-based Intrusion Detection System" or equivalent
- Use scanning software to protect servers from well-known issues and potential unknown vulnerabilities or equivalent
- Make sure all personal computers (each PC/Mac) and local servers (local clients) are HIPAA and FERPA compliant
- Keep usage logs from all equipment on a local server
- Sign a copy of CEI's Technology Confidentiality Agreement.

What conduct and responsibilities regarding data and communications are expected of employees/consultants?

Our members, co-workers, supporters, participants, and consultants entrust CEI with important information relating to their personal lives and businesses. This may include student, personnel and payroll records, CEI business/financial information, policies as well as computer programs and passwords. The nature of the relationship requires maintenance of confidentiality at all times. In safeguarding the information received, CEI earns the respect and trust of our community and of our colleagues.

This principle of confidentiality must be maintained in all programs, departments, functions and activities and applies to release or disclosure in any form of communication (orally, written, digital or any other format). Failure to adhere to this policy is grounds for severe disciplinary action, up to and including termination.

Only employees who have a business reason for CEI and who have been authorized by the Senior Staff will have access to any physical paper records. All physical records will be kept in a locked office or in locked files as reasonable. The files will be locked at a minimum of each night. Sound business practice dictates that the files also will be locked whenever an authorized employee is not present with the files.

All Contractors shall hold CEI-PEA, and each of their directors, officers and employees, harmless from and against all demands, claims, lawsuits, misuse, losses and expenses, arising out of or in connection with this policy as a result of negligence, intentional tort, fraud or criminal conduct or other claim, suit, settlement or other payment (including attorney's fees) on the part of Contractors, and any of its employees, agents, or owners.

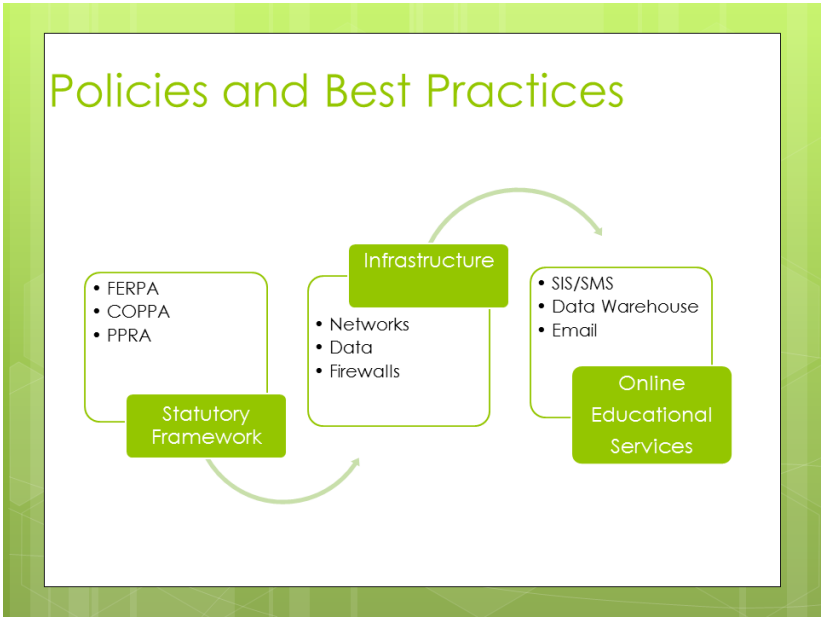
What is the CEI Technology Confidentiality Agreement?

CEI staff relies heavily on its electronic data processing and stand-alone systems to meet its operational, financial,

educational and informational requirements. It is essential that this system and all stand-alone computers/laptops be protected from misuse and be operated in a secure environment. In addition, all computers must be updated with the latest security patches, signatures and data files. CEI may provide a certain amount of its "Confidential Information" to its employees and consultants. For purposes of this Agreement, Confidential Information shall mean, confidential and/or proprietary information of CEI which is not available in the public domain, including but not limited to curriculum and academic materials, personnel records, financial information, and student data, including student names, addresses and academic records. CEI employees, contracted vendors and consultants shall not disclose CEI Confidential Information to any third party. All CEI Confidential Information shall remain the property of CEI and may not be reproduced without the consent of CEI. All digital data files must be returned upon termination of employment or upon the request of CEI. When interacting with New York City Public Schools, adherence to Mayoral Directive No. 81-2 (http://www.nyc.gov/html/careers/downloads/pdf/db_app_guidelines.pdf) is mandatory. Failure to meet the requirements of the Technology Confidentiality Agreement may result in subsequent disciplinary action taken against the employee.

What are some CEI "best practices" to ensure data privacy and security?

- Put your computer into "sleep mode" when unattended
- Change your email password regularly. Do not share it. To ensure a strong, complex password, make sure it includes upper case letter(s), lower case letter(s), numbers, and special symbols (such as $, %, ~, etc.)
- Do not leave any confidential paper files or materials on your desk while unattended
- Do not discuss confidential student information with others; this includes fellow employees unless they have a "need to know" based on their job assignment
- Review CEI's security/privacy policy at least on a bi-annual basis and make necessary changes and adjustments
- Ensure computer is "wiped clean" of data when upgraded or no longer being used.



What action does CEI take if there is a data breach?

The Family Educational Rights and Privacy Act (FERPA) protect personally identifiable information (PII) from

students' education records from unauthorized disclosure. FERPA defines education records as "records that are directly related to a student; and maintained by an educational agency or institution or by a party acting for the agency or institution". FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name). Subject to exceptions, the general rule under FERPA is that an educational institution cannot disclose PII from education records to a provider unless the entity has first obtained written consent from the parents (or from "eligible students," i.e., those who are 18 years of age or older or attending a postsecondary school). Accordingly, the institution must either obtain consent, or ensure that the arrangement with the provider meets one of FERPA's exceptions to the written consent requirement. If there is a suspected breach of such data, the immediate supervisor and the Privacy Officer/President/Superintendent must be notified immediately. According to New York State Bill A 4254, A 3492 notice must also be provided to the Attorney General, the State Consumer Protection Board and the Office of Cyber Security and Critical Infrastructure Coordination. In addition, according to New York City Code 20-117, notice must be provided to the Department of Consumer Affairs and the NYPD.

If a contracted vendor is found guilty of a data breach, employment is ended immediately and notification is made to the proper authorities.

What recommendations does CEI have for school-related stakeholders (school leaders, teachers, parents/families, and students) regarding data privacy and security?

There are a number of laws and regulations regarding data privacy and security that affect school-related stakeholders. These include:

- **FERPA** (Family Educational Rights and Privacy Act) concerns educational records (all records that schools or education agencies maintain about students). It protects the privacy of student education records. It applies to all schools that receive funds under an applicable program of the U.S. Department of Education. (See http://nces.ed.gov/pubs97/97527.pdf).

- **PPRA** (Protection of Pupil Rights Amendment) applies to programs that receive funding from the U.S. Department of Education (ED); it protects the rights of parents and students by seeking to ensure that schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with an ED-funded survey, analysis, or evaluation in which their children participate; and also seeks to ensure that schools and contractors obtain written parental consent before minor students are required to participate in any ED-funded survey, analysis, or evaluation that reveals information concerning 7 specific areas (see http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html)

- **COPPA** (Children's Online Privacy Protection Act) imposes certain requirements on operators of websites or online services directed to children less than 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. See http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

- **CIPA** (Children's Internet Protection Act) Addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. (http://www.fcc.gov/guides/childrens-internet-protection-act)

Each stakeholder group is affected by these laws in different but related ways:

School Leaders

- **FERPA -**
    - School leaders must make student education records available to parents or eligible students for inspection and review.
    - School leaders must consider parental requests to correct student education records that parents believe to be inaccurate or misleading.
    - School leaders must obtain written consent before disclosing a child's personally identifiable information to individuals other than the parent; they are held accountable for restricting inappropriate disclosure of student or parent information.
    - Schools must honor these requests within 45 days of receipt.
    - School leaders are responsible for the overall understanding of privacy regulations and implementation of policies and practices related to education records in schools (federal and state laws as well as local policies outlining parent access to educational records).
    - School leaders must provide annual notification to parents and eligible students of their rights under FERPA. Notification does not need to be individually but must be provided where they are likely to see it (school calendars, websites, etc.)
    - School leaders must make provisions to effectively inform individuals with a disability or whose primary language is not English.
    - If a school discloses directory information (typically student's name, address, phone number, date and place of birth, honors and awards, and dates of attendance), it must give “public notice” of this policy and explain what is included in such information (“Public notice” and means of notification are left up to the school).
    - Notice must also indicate that parents may “opt out” of allowing the school to designate any, or all, of their child’s record as directory information. A model “Notification of Rights under FERPA for Elementary and Secondary Institutions” is available at http://nces.ed.gov/pubs97/97527.pdf.
    - It is important for schools to develop a procedure for assessing outside providers’ contracts to ensure that the provider will comply with the school system’s privacy policies under FERPA, and to provide the school system with some contractual remedies if the provider fails to either meet these standards or comply with applicable law.

PPRA -

- The LEA (local education agency) is required to provide notification to parents and students of their rights under PPRA. It seeks to ensure that schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with an ED-funded survey, analysis, or evaluation in which their children participate.
- The LEA seeks to ensure that schools and contractors obtain written parental consent before minor students are required to participate in any ED-funded survey, analysis, or evaluation that

reveals information concerning 7 specific areas (see http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html).

COPPA -

- School leaders are responsible for ensuring compliance with COPPA. The schools can act as the parent's agent and can consent to the collection of student information when contracting with third-party website operators to offer online programs solely for the benefit of the students and the school system (e.g., homework helplines, web-based testing services).
- School leaders are not permitted to act on a parent's behalf if the online service plans to use children's personal information for purposes outside of the agreed learning experience.
- School leaders should provide parents with a notice of the online services it will be using and what personal information about students they have provided to service providers on their behalf, and the websites' individual practices on sharing and collecting personal information with parents.
- School leaders should have a process for assessing sites' and services' practices related to online privacy. (http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions)

CIPA -

- School leaders must educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.
- School leaders must ensure that policies, rules and guidelines related to filtering should be created through a formal, collaborative process undertaken by a group consisting of teachers, students, technicians and community members. Such a group can address the issues (i.e., what filter to use, process for approving requests to block/unblock sites, who has the authority to override the filter, and how the effectiveness of the filtering policies should be evaluated) and make recommendations to administration.

Teachers

FERPA -

- Teachers cannot disclose education records (including student addresses and/or telephone numbers) to other students.
- Teachers should not "click through" a Terms of Service agreement without reading it to gain access to technological tools, as that action can bind the school to terms that do not align with security protocols and policies, and can put the school system at legal risk if the provider's practices fail to comply with privacy laws that apply.
- Teachers should be aware grades on peer-reviewed papers before they are collected and recorded, as well as personal notes, are NOT considered to be education records and as a result do not fall under FERPA restrictions.

COPPA -

- The FTC recommends that schools or school districts decide whether a particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher.

CIPA -

- Teachers frequently are given responsibility 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. (A quality resource is the Common Sense Media Toolkit on CIPA for teachers at https://www.commonsensemedia.org/educators/erate-teachers

Best practices for teachers:

- Do not assume that every school employee is entitled access to student educational records or demographic information. Access must be for appropriate purposes - part of the professional duties of the person to whom the records are being disclosed. (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/safeguarding-student-privacy.pdf)
- Do not contract with online educational service (OES) providers for their services. Teachers frequently do so, however, if the service is free. The US Department of Education recommends teachers "not bypass internal controls in the acquisition process when deciding to use free online educational services" (i.e., whatever system of approval is in place for the use of paid OES should also be used for free OES). http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf
- Do not make light of Terms of Service (TOS) agreements. Many OES providers require one to click to accept their TOS. With "click-wrap" agreements, the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to signing a contract. As with the previous bullet, teachers should go through the school's system of approval prior to clicking, in order to protect the privacy and security of students. http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20(February%202014).pdf

Parents/families

FERPA -

- Parents have the right to inspect and review (but not to receive copies, except in limited circumstances) their child's education record.
- Parents can request that a school correct records which they believe to be inaccurate or misleading under limited circumstances.

(Note - Parents whose children receive services under the Individuals with Disabilities Education Act **(IDEA)** may have additional rights)

PPRA -

- Parents have the right to inspect any material used by students in ED funded surveys, analyses, or evaluations prior to use with their child.
- Parents' consent must be received before a minor student is required to participate in ED funded surveys, analyses or evaluations which may reveal personal information; parents have the choice to opt their child out of sharing such information with the school.

COPPA -

- Requires operators of commercial websites and online services to provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children.
- Gives 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).
- Requires operators of commercial websites and online services to:
    - provide parents access to their child's personal information to review and/or have the information deleted
    - give parents the opportunity to prevent further use or online collection of a child's personal information
    - 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
      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.

Students

FERPA -

- When a student turns **18 years old** or enters a postsecondary institution at any age, **all rights afforded to a parent under FERPA transfer to the student**. (However, FERPA provides ways in which a school may - but is not required to - share information from an eligible student's education records with parents, without the student's consent).

PPRA –

- The Local Education Agency is required to provide parents and students with information about their rights and protection when instructional materials and student evaluations are used in an ED-funded survey, analysis, or evaluation. It ensures that students and their parents will be kept safe and therefore have the right to inquire about terminology used in materials as well as explanations. Stakeholders will be informed of state, local and federal laws, policies, regulations and best practices as pertaining to PPRA.

APPENDIX

Disclaimer of Liability

Neither CEI, nor any of its employees, agents or individual board members, shall be held liable for any improper or incorrect use of the information described and/or contained in our sites and assumes no responsibility for anyone's use of the information. In no event shall the CEI, or its employees, agents or individual board members be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement or substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this system, even if advised of the possibility of such damage. This disclaimer of liability applies to any damages or injury, including but not limited to those caused by any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, communication line failure, theft or destruction or unauthorized access to, alteration of, or use of record, whether for breach of contract, tortious behavior, negligence or under any other cause of action.

Disclaimer of Warranties and Accuracy of Data

CEI's websites do not contain any data that targets individual teacher or student personal information. CEI's Children's First Network (CFN) schools are located under the auspices of the NYC Department of Education (DOE) and therefore are covered by the DOE's Privacy/Security Policies. CEI may provide access to student data to contracted Data Warehouses. These companies have been investigated and uphold the highest standards in protecting student/teacher data. CEI may provide this information on an "as is" basis. All warranties of any kind, expressed or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, freedom from contamination by computer viruses and non-infringement of proprietary rights are disclaimed.

Any inappropriate activity should be relayed to the Director of Human Resources at 212 302 8800.

Disclaimer for External Links

CEI's websites include links to other sites. These include links to sites operated by other agencies and officials, other government agencies, nonprofit organizations and private businesses. When a user leaves the CEI's website and visits another site, the user is subject to the privacy policy of that new site. CEI is not responsible for the contents of any off-site pages referenced. The user specifically acknowledges that CEI is not liable for the defamatory, negligent, inaccurate, offensive, or illegal conduct of other users, links, or third parties and that the risk of injury from the foregoing rests entirely with the user. Links from CEI web pages to other sites do not constitute an endorsement from CEI. These links are provided as an information service only. It is the responsibility of the user to evaluate the content and usefulness of information obtained from other sites. CEI's websites contain links to other related sites and resources. Since CEI is not responsible for the availability of these outside resources or their contents, the user should direct any concerns regarding any external link to its site administrator or webmaster.

Privacy Policy Changes

Although most changes are likely to be minor, CEI may change its Privacy Policy from time to time, and in CEIs' sole discretion. CEI encourages visitors to frequently check this page (www.thecei-pea.org) for any changes to its

Privacy Policy. Your continued use of this site after any change in this Privacy Policy will constitute your acceptance of such change.