Privacy and Security in CLIC

A consensus is emerging among privacy experts that technology solutions themselves must, by design, protect private information and keep it secure from accidental disclosure. Privacy by design places the onus for protecting private information on technology developers and decision-makers rather than on students and teachers. Pearson's privacy solution is embracing that responsibility. This paper considers the challenge of protecting private information in a cloud-based world and describes the privacy and security measures provided by CLIC, a web-based tool for documenting learning in classrooms.

The Challenge

Educational institutions are expanding their use of online learning technology. This evolution delivers clear benefits for students, instructors, parents, and administrators. Digital assessment tools can automate many time-consuming tasks of classroom administration, freeing teachers to spend more time interacting with students and providing individualized plans that personalize learning experiences for each student.

Increasingly, today's educational technology solutions are web-based. The Internet has become the dominant delivery system for applications and services. Given the increasing ease of accessing the Internet from anywhere at any time, from fixed and mobile computers and devices, web-based education tools will continue to grow in use.

The ubiquity of the Internet has enabled the delivery of a growing number of technology solutions from "the cloud." The cloud, in this context, refers to web-based technology solutions that are hosted and managed by the solution providers as a service, rather than being deployed locally by individual institutions.

There are many benefits to this cloud-based approach. There is an economic benefit: it is less expensive to maintain a centralized data centre that serves all users than it is to deploy many installations that serve smaller groups of users. Another significant benefit is scale and performance: one robust data centre, with best-in-class security measures, hardware and software redundancy, and disaster recovery measures can outperform dozens of smaller centres. Given the clear economic and performance advantages, more and more of today's education technology solutions are cloud-based.

Maintaining the security of the information stored within technology solutions is a priority. Protecting sensitive personal information is paramount. Just as medical information is considered private and must be safeguarded, education data contains sensitive elements that require effective security protocols. Because protecting electronic data can be extremely complex, the privacy and security concerns around electronic information are especially acute.

Who Manages Privacy within an Institution or Province?

It is important to examine the human context in which educational technologies are selected and deployed. For example, in Ontario, with the approval of the Council of Directors of Education, the Privacy and Information Management (PIM) Taskforce (www.pimedu.org) supports the development of an information management culture to respect privacy in the province. One goal: to find the balance between operational efficiency, providing educational services, and protecting privacy. All school districts have designated a Senior Administrative PIM Champion responsible for overseeing local school district implementation. Each district has also identified a cross-organizational local implementation team and developed an approach to the role based on local privacy and information management culture and needs.

The role of the PIM Champion is to

- Champion privacy and information management issues within their school district
- Understand MFIPPA and the Education Act
- Represent the district in partnership discussions relevant to privacy and information management
- Bring to bear insights into privacy and information management on the development and delivery of the district's services and policies
- Create a cross-organizational team to advocate privacy concerns and ensure that the district's privacy policies are embedded in daily practice

What Exactly is Personally Identifiable Information?

Although variations in the definitions of personal information exist among privacy laws, personal information generally includes any information unique to an individual, such as their home address, opinions, educational records, age, gender, income, medical records, and financial data.

Some personal information is deemed to be in the custody of a public body, like educational records in the custody of a school or medical records in the custody of a hospital.

Anonymous data, i.e., data not identified or linked to an individual by name, is not personally identifying information. Personal information does not usually include employee contact information.

Canadian Privacy Laws

FEDERAL LAWS

Canada has two federal privacy laws: the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA).

The Privacy Act imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use, and disclosure of personal information. Individuals are also protected by the Personal Information Protection and Electronic Documents Act that sets out rules for how private sector organizations may collect, use, or disclose personal information in the course of commercial activities. The law gives individuals the right to access and request correction of the personal information these organizations may have collected about them. It obliges organizations to protect and limit access to personal information and provide a ready means for individuals to review, alter, or remove their personal information. Oversight of both federal Acts rests with the Privacy Commissioner of Canada who is authorized to receive and investigate complaints.

PROVINCIAL LAWS

Each Canadian province has laws to protect and govern the gathering, storage, and use of personal information. Of particular relevance to educational institutions are British Columbia's privacy laws, as well as those of Nova Scotia, because these two provinces have enacted some of the strictest guidelines in the country.

British Columbia's two principal laws are the: Freedom of Information and Protection of Privacy Act (FIPPA) and Personal Information Protection Act (PIPA). FIPPA allows access to information held by public bodies (such as ministries, universities, and hospitals) and determines how public bodies may collect, use and disclose personal information. PIPA sets out how private organizations (including businesses, charities, associations, and labour organizations) may collect, use, and disclose personal information.

Under FIPPA, personal information that is in the custody of a public institution, e.g., schools, colleges, and universities, must reside on a server in Canada, unless consent is obtained from the individuals for it to reside elsewhere.

The relevant legislation in Nova Scotia is the Freedom of Information and Protection of Privacy Act, which applies to provincial and local public bodies, including community colleges, schools, and universities, and the Personal Information International Disclosure Act, which prohibits access to or storage of personal information outside Canada if the personal information is in the custody or under the control of a public body, without explicit consent of the individuals or under particular circumstances, such as meeting requirements of the public body's operation.

Privacy by Design

Developed by Ontario Information and Privacy Commissioner Dr. Ann Cavoukian, Privacy by Design advances the view that privacy cannot be assured solely by compliance with legislation and regulatory frameworks, but that privacy assurance must become an organization's default mode of operation.

Dr. Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of Privacy by Design seeks to proactively embed privacy into the design specifications of information technology and business practices, thereby achieving the strongest protection possible. In October 2010, regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing Privacy by Design as an essential component of fundamental privacy protection. This was followed by the United States Federal Trade Commission's inclusion of Privacy by Design as one of its three recommended practices for protecting online privacy—a major validation of its significance.

What is CLIC?

CLIC (Capturing Learning in the Classroom) is a Canadian-developed, web-based tool that allows teachers to:

1. **Capture observations**
   Teachers can use any device to capture their observations: digital cameras, video cameras, phones or tablets. Photos, videos, or audio recordings can be uploaded to CLIC. If teachers are using a tablet, they can even capture their notes directly in CLIC.
2. **Build Learning Stories**
   The Learning Story template in CLIC allows teachers to easily upload files and connect children to the story. They can also input their observation notes, record their reflections on the observation, and capture their ideas for extending learning at school and at home.
3. **Connect to Curriculum**
   The Learning Story template also allows teachers to easily connect the learning story to their curriculum outcomes/expectations. They can also record the level of skill development for individual children connected to the learning story.
4. **Generate Summaries**
   CLIC automatically generates a variety of individual and class summaries that allow teachers to analyse their observations. These summaries are a great support when planning for and reporting on learning.
5. **Communicate with Parents**
   With CLIC, teachers can easily share learning stories with parents either by emailing learning stories directly to parents or by providing a link to a secure website where parents can view their child's learning stories. This home communication feature is an efficient way of informing parents what their child is learning and how they can support learning at home.

Privacy Provisions in CLIC

Throughout the development of CLIC, privacy and security was an overriding consideration. The following provisions in CLIC will help protect the privacy of your students.

Where is data in CLIC stored?

Data uploaded or entered into CLIC is not stored on individual computers or mobile devices. Rather, data is stored centrally in a secure environment on a network server. Districts may choose to host CLIC on their district server or have Pearson host CLIC on its server located in Canada. Both hosting options mean that no data is stored outside Canada and is, therefore, subject to Canadian privacy legislation.

Who has access to the personal information in CLIC?

There are three levels of administration associated with any CLIC implementation. Following is a summary of information that is accessible at each level.

License Set-Up (Pearson Canada)

Regardless of whether CLIC is hosted locally by a school or district or hosted by Pearson, members of the Pearson Canada Digital Support Team will have access to the name and contact information (address, email, phone number) of the License Administrator(s) appointed by the purchasing school or district. No personal information in CLIC can be accessed or viewed by any employee of Pearson Canada.

License Administrator(s)
(District or School Appointed Personnel)

A License Administrator coordinates the installation and/or set-up of CLIC and the entry or upload of classroom, teacher and student information. They will have access to student information including name, birth date, parent/guardian contact information and teacher information including name, school, phone number, email address, and the students in their class. They can not access or view any other data in CLIC.

License Use
(Teachers or Early Childhood Educators)

When a License Administrator set-ups a teacher, the teacher receives an email requesting they register by setting a password for their account. Once set, only the teacher knows that password – it is not made available to Pearson or the License Administrator. Once their account is activated, they will have access to or can input student information including name, birth date, parent/guardian contact information for only the students in their classroom. They will also be able to create learning stories that include photos, video, audio, and written comments pertaining to their students. Only the teacher(s) connected to the classroom have access to these learning stories.

How is personal information in CLIC protected?

All data in CLIC is password protected. Having this strict protocol ensures that the various people involved in a CLIC implementation have access to only the information they are authorized to access.

Data is stored using AES (Advanced Encryption Standard) or 3DES (Triple Data Encryption Algorithm) to protect it from being read by anyone not authorized to access the files, including server administrators. This is the same type of encryption used by many government, healthcare and law enforcement agencies.

Can information in CLIC be shared?

CLIC does allow learning stories to be shared at the discretion of the teacher. There are a number of reasons why a teacher might want to share learning stories.

- They may want to print out learning stories to post in the classroom so children can celebrate their learning.
- They may want to print out a learning story for reference during a teacher/parent conference or a teacher/student conference.
- They may want to communicate learning stories with parents so they are kept informed of their child’s development.
- They may want to share learning stories with other educators connected to a child’s education (principals, resource teachers, occupational therapists, speech and language pathologists, etc.)

It is the responsibility of the purchasing district or school to establish, communicate, and enforce a permissions policy. This policy relates to the need for parents or guardians to give consent for learning stories (which may include written comments, photographs, video, and audio recordings) of their children to be captured and/or shared. Learning stories will often include groups of children and parents should understand that these learning stories might be shared with parents of other children in the group.

CLIC allows for learning stories to be output in a variety of ways to address the various reasons why teachers may want to share learning stories. However, there are a number of safeguards built into CLIC that will ensure teachers are informed of any restrictions imposed by parents or guardians whenever they attempt to share a learning story.

In the Student Information section of CLIC, teachers must indicate whether they have received consent from parents or guardians. The default setting for receiving consent is set by CLIC at “No.” Teachers must change the setting to “Yes” when such consent is received. The purchasing district or school is responsible to decide if they will require specific parent/guardian consent for children to participate in CLIC and the wording of such consent (a sample consent form is provided in CLIC that can be used or adapted).

If consent has not been received for a student or if there are any restrictions imposed by parents or guardians, the teacher leaves the consent set to “No” and can input comments which detail any restrictions. A flag will appear when a child, for whom consent has not been received, is connected to a Learning Story.

An alert will appear when a child, for whom consent has not been received, is connected to a Learning Story selected for printing, emailing or viewing (by anyone other than the teacher). This alert will prompt teachers to consider whether proceeding will in any way be in violation of the restriction placed against the child or children for whom consent has not been received.

Through CLIC, teachers have the ability to email learning stories to parents/guardians or email a link to a protected website where parents/guardians can view the learning stories of their child. During CLIC set-up, the License Administrator can disable this Home Connection so that no learning stories can be sent from CLIC. If the Home Connection is enabled, teachers can choose not to include photographs, video, or audio when sharing Learning Stories and can edit or revise the learning story that is shared. CLIC will automatically issue the following reminder with every Learning Story that is shared:

> Please remember: Privacy matters. This learning story might include written comments, photographs, audio, or video of children other than your own. Please do not repost any of this content online.

Conclusions

After careful consideration of the challenges surrounding the protection of private information in a cloud-based environment, Pearson believes that privacy protections should be designed into the technologies themselves. This privacy-by- design approach enables education officials to select best-of- breed learning solutions such as CLIC with the assurance that private information will be kept securely private. The privacy and security measures described in this paper keeps Canadian students' information locked and encrypted within Canada and ensures teachers can make informed decisions when sharing information.

Pearson Canada
For more information, please contact us:
26 Prince Andrew Place
Don Mills, Ontario M3C 2T8
416-447-5101
1-800-263-9965
416-443-0948 (fax)
www.pearsoncanada.ca