

1. Specifying Purposes

1.1 Providers must state all data elements that their classroom web apps or services collect and provide reasons for the collection/processing of each element.

2. Consent

2.1 Schools must ensure there is verifiable parental consent for the collection, use and disclosure of personal information of children under 18 if there is no legal basis for using classroom web apps/software/services as determined by law or established by regulators.

2.2 Unless consent is obtained, providers must allow students to maintain ownership of and be in control of the content they create and upload to the classroom web app/software/service.

2.3 Providers must offer consent options so that users (or parents/guardians) can consent to the collection and use of personal information necessary to provide the service without consenting to the use or disclosure of that information to third parties for other purposes (e.g., marketing).

3. Collection

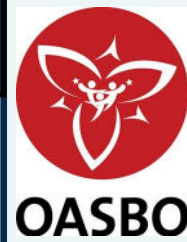
3.1 Providers must collect only the personal information required to operate the classroom web app/software/service, e.g., no accessing browser history, contact lists, search terms, preferences, device identification, location, etc. unless directly related to providing the service.

3.2 When apps are to be downloaded onto mobile devices, providers must offer choices to users regarding disclosure of data on their device such as location, identifiers, contacts, etc.

3.3 Providers must never collect personal information covertly, i.e., without the user's knowledge, particularly audio/video information via the user's own device.

3.4 Student profiles and activity within the web app or service must be kept private so that they cannot be seen or collected by others unless the app/service itself is collaborative and requires this type of sharing.

3.5 Educators should be allowed to create generic accounts for children (e.g., student 1, student 2, etc.) and/or create profiles using as little personal information as possible in order to avoid the excessive collection of personal information.



OASBO



STUDENT DIGITAL
PRIVACY STANDARD
for

Classroom Applications, Software and Web Services

To ensure that web apps, software and online services used in Ontario school boards adhere to uncompromising high standards of protection, these criteria are based on data protections for children endorsed by regulators and experts across North America and the European Union. This standard is intended to shift the data protection landscape and raise the bar for student digital privacy in Ontario schools.

4. Use, Retention, Disclosure

4.1 Providers must use, disclose and retain personal information only for the purpose of providing the classroom web app/software/service.

4.2 Providers must not benefit or profit from student personal information.

4.3 Providers must not profile children for marketing purposes or in ways that lead to unfair, unethical or discriminatory treatment.

4.4 Providers must not repurpose student data or use it for research without express consent, unless authorized by statute or anonymized.

4.5 Providers must securely destroy or make anonymous in a timely manner all personal information that is no longer required to provide the app/software/service and they must explicitly identify retention timelines.

5. Security Safeguards

5.1 The provider must have a comprehensive security program in place that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks, (e.g., unauthorized access or use, unintended or inappropriate disclosure) through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

5.2 Providers must define the safeguards in place.

5.3 Providers must ensure that all vendors they use to provide the service implement the same security safeguards.

5.4 Providers must ensure that all successor entities are obligated to implement the same security safeguards for personal information previously collected.

5.5 Providers must have breach protocols in place.

6. Openness and Transparency

6.1 Providers must communicate privacy notices, terms of use, contracts etc., in clear, specific and unambiguous language that explains to users how their personal information is being used, processed, disclosed and retained by the provider and any third parties.

6.2 Providers must make links to privacy policies and terms of use, etc., easy to find after the account has been created.

6.3 Providers must identify the third parties to which they disclose personal information for processing, the specific data elements involved, and a summary of protections/assurances in place.

6.4 Where providers use data for statistical analysis and profiling, for making subjective assessments, for predicting behaviour or as part of a decision-making process it should be clearly communicated by providers to users along with a mechanism to challenge these assessments.

6.5 Providers must state whether or not the classroom app/service allows users to make personal information publicly available online.

6.6 Providers must directly inform users before changes are made to policies and terms of use, etc., before data is used in a manner inconsistent with the terms they were initially provided.

6.7 Providers must disclose the presence and use of third party cookies and provide options for managing them.

6.8 Provider must confirm that they are in compliance with all laws.

7. Access and Correction

7.1 Providers must make available the name and contact information of an operator who will respond to inquiries and challenges from users or parents/guardians about privacy policies, data handling practices, accuracy, completeness and use of personal information.

7.2 Providers must have a mechanism for users to access, correct, erase, and download content they created in a useable format.

7.3 Users have the right to erasure of their data, including metadata inferences, assessments and profiles (if not required for administrative purposes by the provider or the school board) and providers will not charge a fee for this service.

7.4 Providers must ensure that when a student deletes their work in their account created by an educator where the educator maintains exclusive administrative rights, the copies in the educator account must disappear, also.

7.5 Providers must ensure that educators have the ability to delete their own accounts and virtual classrooms.

7.6 Providers must not require users to surrender their copyright to their own work if they post it to the application or service's site.