Analysis of Student Data Privacy Compliance in Ontario High Schools

Alignment of EdTech Practices with MFIPPA, Bill 194, and Related Legislation

Prepared by: Josiah Pinheiro
Independent Researcher

Ontario, Canada
January 2026

Statement of Research: Analysis of Student Data Privacy Compliance in Ontario High Schools

Question: Are EdTech Practices aligned with MFIPPA, Bill 194, etc?

Research Objective: This research analyzes how EdTech platforms in Ontario school boards collect, store, and share student data. It aims to find any differences between the platforms' policies and the requirements mandated by Ontario's Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Bill 194 (2024).

Legal Framework / Ontario Student Data Protection

Legislation	**Why**
MFIPPA (Municipal Freedom of Information and Protection of Privacy Act)	Forces school boards to only collect what they need for class.
The Education Act & OSR Guidelines	Forces official school records to be used only to improve instruction.
Bill 194	It requires boards to check all their AI tools for vulnerabilities and notify you if there is a data breach.
Pipeda	Stops private companies (Google/Kahoot) from using your data for things like ads.
Digital Privacy Charter	Enforces the rule that the highest privacy settings should be on by default.

Platform Compliance

Platform	**Data Collected (Policy Claim)**	**Practice**	**Relevant Law**
School Board Website	IP, cookies, analytics	Uses Google Analytics → third-party data transfer	MFIPPA / PIPEDA
Brightspace (D2L)	Grades, submissions, usage data	Tracks engagement metadata	MFIPPA / Bill 194
PowerSchool	Student records, attendance	Long-term retention → breach exposure	MFIPPA / Education Act
Google Classroom	Account + activity data	Metadata collection across services	PIPEDA

Brightspace

Brightspace by D2L collects the information that's required for the platform, like usernames, emails, etc. Brightspace also gathers data through cookies and other tools. When school boards use Brightspace, they input student data like attendance and grades, and this means that a variety of student information lives in Brightspace. D2L, which owns Brightspace, have policies which state that the users (schools), have ownership of this data. They go further, saying D2L will not use student information for any other unknown or 2nd purpose. D2L asserts compliance with Canadian privacy standards by following and submitting to PIPEDA, being a signatory of the Student Privacy Pledge, and by staying/being in alignment with Canadian privacy rules.

Brightspace has not been involved in any significant privacy breaches thus far, but when talking about cloud-based education platforms, a robust and intelligent security approach is more than just necessary. The Information and Privacy Commissioner of Ontario has pointed out that because school boards operate under MFIPPA, they are obligated to, and must have, strong safeguards for student personal information.

Investigations focusing on similar e-learning platforms revealed something important. When these security measures are clearly stated in contracts, the school boards have the responsibility to actively keep tabs on the vendor's security habits. This goes beyond simply preventing the obvious data breaches and vulnerabilities. For platforms like Brightspace, school boards need to conduct regular reviews and ensure that every single thing lines up with MFIPPA. We are talking about student data, how it is collected, how it is handled, etc. It is quite the task to make certain that you are in alignment with every aspect contained in MFIPPA. There is a lot to get through, and sometimes it is difficult to know exactly what is what.

To sum up, Brightspace's data handling practices are in line with Ontario's requirements. It complies with MFIPPA and has done well to protect its students and data. D2L has obeyed local laws, maintained certifications (ISO 27001/27701), and asserted its compliance, showing how committed it is to following standards and cybersecurity rules. However, school boards are still 100% responsible for making sure that Brightspace is being used in a way that is compliant with MFIPPA. Keeping parents informed and helping protect student privacy is critical.

PowerSchool

PowerSchool is a system that takes the personal data of students and staff and centralizes it. From their policies and recent incidents, it is true that PowerSchool holds student names, contact information, dates of birth, even medical records, and more. This platform uses this information to help direct and operate enrollment systems, grades, attendance and etc.

In late 2024, PowerSchool was hit with a massive cyberattack that essentially exposed all of this sensitive and critical information. 3.86 million people in Ontario and other provinces were affected. Privacy commissioners in Ontario launched an investigation. They discovered that a criminal somehow got one of the admin's emails and passwords. Multi-factor authentication was missing, and always-on remote support access was left enabled on the system! The incident only got worse by the second because nobody was monitoring the systems, and the breach detection system was not up to par. The school boards that were affected by this breach barely had an incident response plan, with one board having no response plan at all. It was also found that the boards genuinely had not included the security clauses in their agreements with PowerSchool. They were also not making regular oversight of the vendor’s practices. These were all violations of the many boards’ obligations to protect their information.

MFIPPA states that school boards must protect the crucial information of students that is in their custody and prevent unauthorized access or disclosure. The privacy commissioner's report on the incident stated that the boards did not have reasonable measures to secure the data. This breach raised concerns and ignited the search for non-compliance with MFIPPA and other security requirements and laws. The duty to keep critical information was taken lightly, but it also showed gaps in post-breach incidents. School boards governed by MFIPPA had no statutory mandate to report breaches or to assess risks. Bill 194 was updated to include mandatory breach notification and more/other cybersecurity safety measures. PowerSchool did voluntarily notify affected individuals, and contract and law compliance have certainly changed since then. PowerSchool handles highly confidential student information, so compliance with MFIPPA is non-negotiable.

Google Classroom

Google Classroom is in the Google Workspace for Education suite, and the Google Workspace for Education suite is very prominent, being largely used by many schools in Canada. Google Classroom collects personal information about the students and the educators (emails, names, etc). Google is firm in its policy, stating that it only acts as the processor of the data. So the school board keeps control of the data, not Google. Google also say that they don't scan student data for advertising at all. Despite this, privacy concerns were raised when a privacy commissioner examined if a school board's use of Google's G Suite for education was compliant with MFIPPS. No breach of laws was found, but areas of improvement were evident.

The privacy commissioner recommended that the boards be very clear and transparent in telling parents and students the personal information that Google collects, and even why it's collected. Names, emails, and assignments need to all be within the parents' knowledge. This will improve notices of collection, bringing more understanding to everybody involved. It was also recommended that the school boards be very rigorous and consistent in monitoring the privacy policies and practices of Google. Any changes to its policies and practices need to be followed up on by the board, its staff team, etc. Even though Google provides the service, the school board will still be 100% liable and responsible for the student data. Under MFIPPA, school boards can allow student data to be collected, must limit data to what's necessary for education, must inform about their collection and related practices, and must keep the data SAFE. Because these boards are using Google Classroom at this scale, they are automatically required to conduct privacy risk assessments and must keep everything in order, making constant reviews and follow-ups with any changes, and most importantly, they must keep the data safe.

Google is subject to PIPEDA, meaning that Google must protect personal information. Google is also obligated to use this information with the utmost proper consent and apply robust, quality safeguards to keep this information from bad actors. Google uses encryption, regional data storage, and more to ensure that this is happening. Google has also signed important agreements like the Student Privacy Pledge, showing its commitment to keeping such information safeguarded. Google Classroom can be compliant with the MFIPPA and the PIPEDA, but constant reviewing and monitoring are essential.

Public School Board Websites

Ontario school board websites collect personal information in limited ways. They collect this info through forms, registrations, feedback, and more. The information they collect is very basic, usually including things such as names, phone numbers, etc. MFIPPA states that school boards can only collect what is necessary and explain the reason why they're collecting it. The majority of school boards include their privacy statements on their websites. One board, for instance, the Bluewater District School Board, states on their website that the personal information is used for its intended purpose only, and that the information is not shared with any third parties at all without consent. Boards acknowledge their duty and responsibility to protect information and comply with laws like MFIPPA.

Despite this, multiple upon multiple school boards in Ontario have gone through significant cyber attacks ranging from ransomware to data breaches. In many cases, crucial personal information was exposed. Privacy commissioners have shown that many boards genuinely have low security, and many have a weak or even no response plan in place, as seen with the incident in 2024.

MFIPPA needs boards to actually protect information, but it actually doesn't require school boards to report on breaches, to conduct impact assessments, or to automatically notify affected individuals. Ontario's Privacy Commissioner has urged the government to make the MFIPPA a bit more rigorous to mandate stronger practices, like the practices and standards of FIPPA. Bill 194 introduced a lot of stronger and more robust practices in cybersecurity, yet they don't apply to school boards. Boards are not required to report on breaches, yet some boards voluntarily report on breaches and build trust with families.

Conclusion

In essence, Google Classroom and schoolboard websites can be used safely if school boards simply do their part. School boards need to be transparent with everything, collect only the required data, and keep this data safe. Even things like staying informed on new changes in technology are expected. When you're in charge of the data of millions of people, you'd better be willing to put in the work. And so, while current laws like MFIPPA set the basic requirements, new threats and developments in technology and AI show that stronger standards and policies are essential. It's not about not getting information leaked. It's about upholding that trust with everyone else.

Sources

1. **MFIPPA – Municipal Freedom of Information and Protection of Privacy Act (Ontario)**

   https://www.ontario.ca/laws/statute/90m56

2. **Bill 194 – Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024**

   Ontario Government Summary: https://www.ontario.ca/page/strengthening-cyber-security-and-building-trust

3. **PIPEDA – Personal Information Protection and Electronic Documents Act (Federal)**

   https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

4. **Information and Privacy Commissioner of Ontario – Guidance on Education Privacy**

   https://www.ipc.on.ca/privacy/education/

5. **PowerSchool Privacy Breach – IPC Joint Report (Nov 2025)**

   https://www.ipc.on.ca/newsrelease/ipc-psp-report-student-privacy-2025/

6. **D2L Brightspace Privacy Policy**

   https://www.d2l.com/legal/privacy/

7. **Google Workspace for Education Privacy Notice**

   https://edu.google.com/intl/en_ca/why-google/privacy-security/

8. **Google Education – Trust Center**

   https://edu.google.com/why-google/privacy-security/

9. **Ontario Education Act – Student Record Regulations**

https://www.ontario.ca/laws/statute/90e02

10. **Student Privacy Pledge – D2L, Google, PowerSchool Signatories**

    https://studentprivacypledge.org/

11. **TDSB (Toronto District School Board) Notice of Collection**

    https://www.tdsb.on.ca/About-Us/Policies-Procedures-Forms/Privacy-Information

12. **Bluewater District School Board – Website Privacy Statement**

    https://www.bwdsb.on.ca/privacy

13. **Ontario Privacy Commissioner – Public Statements on MFIPPA Gaps**

    https://www.ipc.on.ca/newsrelease/mfippa-breach-report-2025/

14. **Upper Canada District School Board Breach Notification (2025)**

    https://www.ucdsb.on.ca/news/2025-breach-response

15. **CBC News – PowerSchool Data Breach Ontario Coverage**

    https://www.cbc.ca/news/canada/powerschool-breach-ontario-2025