FillmoreRiley

MSBA 2026 Convention
FIPPA Update
March 20, 2026

Presented by: Paul K. Grower & Morgan Whiteway

PURPOSE OF FIPPA

- “to allow any person a right of access to records in the custody or under the control of public bodies, subject to the limited and specific exceptions set out in this Act”
- “to allow individuals a right of access to records containing personal information about themselves in the custody or under the control of public bodies, subject to …”
- *right to request corrections*
- “to control the manner in which public bodies may collect personal information from individuals and to protect individuals against unauthorized use or disclosure of personal information by public bodies”
- *Independent review*

NOTES

PAUL'S PRIVACY PRINCIPLES

- The best interests of the students will ALWAYS prevail
- We CAN dispute Ombudsman's decision in Court or force them to make THE decision
- Always try to show good faith
  - Consult – lawyers / others – NO LONGER GHOST WRITE
    - Media raised concerns and "looks like it was lawyered"
  - Don't automatically disclose – GO UP ONE LEVEL AND ASK
  - Emergencies – health and safety are an exception
    - KEEP DISCLOSURE TO MINIMUM – Don't be convinced to "talk" – **COPS!!**
    - BUT REPORT UP A LEVEL AFTERWARDS
- Is it better to refuse access to start? Often, YES!
- Not limited to initial FIPPA position to applicant with Ombudsman
- ALWAYS READ AND RE-READ THE PROVISIONS OF FIPPA

WHEN A REQUEST COMES IN….

- FIPPA request does not need to be on prescribed form (s.8)
  - Oral request can be made where applicant has limited ability to read or write in English or French, or has disability or condition (s.8(3))
- If unclear, ASK the applicant what they want
  - Duty to assist (s.9)
  - ***Consider additional information request*** (s.12.1) – puts response time "on hold" until they reply – and they only have 30 days to reply (but are to be notified that application then considered abandoned)

- **Parents - *We will respond in accordance with FIPPA/PSA***
  - ***Triggers rights / obligations / timelines***

The Public Schools Act

- "Pupil File" means a record or a collection of records respecting a pupil's attendance, academic achievement and other related matters in the possession or control of a school board
- s.42.3(1) on request, the school board MUST provide pupil file to parent, or, pupil (if pupil has reached age of majority)
  - In latter case, cannot disclosure to parent w/o consent of pupil
- s.42.3(2) MAY refuse access to all or part of pupil file where disclosure could reasonably be expected to:
  - (a) constitute an unreasonable invasion of the privacy of a third party
  - (b) be detrimental to the education of the pupil;
  - (c) cause serious physical/emotional harm to the pupil or another person
  - (d) injurious to enforcement of enactment / investigation under enactment

The Pupil File

- What is it?
  - Broad definition
  - What do we put in it? → handwritten notes (**then**) v. emails (**now**)
  - Where is it kept? – teacher records / counsellor records / office records
- Be aware of devices (personal or Division) – texts, etc. are often NOT saved like emails
  - "Don't forget your cleats" v. abuse issues
  - Move to email communication?
  - Screenshots (noting you may not be able to do a text search)?

NOTES

The Pupil File

- PRESUME WHAT YOU PUT IN WRITING WILL BE REVIEWED
  - Use “counsellor” speak / quote verbatim
- **BUT NO MATTER WHAT – STILL DOCUMENT! - TEXTING**
- While you can trigger FIPPA to set timelines, etc. …
- Relying solely on FIPPA to deny pupil file is really not possible
  - Refusing pupil file disclosure VERY difficult
    - Third party privacy – redact
    - Detrimental to education of pupil – HARD TO KEEP FROM PARENTS
  - Need an objective opinion by **NOT CONNECTED** professional
    - “cause serious physical/emotional harm to the pupil or another person”
    - what if pupil harms selves later… risks of not giving access
  - Watch parent just “showing up” to review the pupil file

PowerSchool Incident

- Late 2024 cybersecurity incident compromising data in the Student Information System
- Someone stole “credentials” of PS staff member – access SISs via maintenance protocols
  - Both internally stored and cloud-stored SISs impacted
- Impacted millions of individuals (students, staff, parents, etc.)
  - Students – names, ID, DOB, contact / family law / medical info, PHIN
  - Staff – names, contact, SINs
  - Parents – names, contact, family law info

PowerSchool Incident – AB / ONT Findings

- Failed to include sufficient privacy / security provisions in the agreements with PS to meet provincial law
- Lacked policies / procedures to monitor and oversee PS's security safeguards to ensure compliance with contractual terms (e.g. MFA)
- Failed to limit remote access by PS to limited periods
- Lacked adequate breach response plans

FROM THE OMBUDSMAN WEBSITE

Educational technologies have become deeply embedded in the way that education is delivered. They are now a central feature of Canadian classrooms particularly since their adoption increased exponentially during the COVID-19 pandemic.

EdTech includes technologies that support curriculum delivery, content engagement, attendance, and testing and assessment of students in elementary, secondary and post-secondary institutions.

However, they can also introduce new risks to privacy — especially for children and young people who have no choice but to use educational platforms that collect and use their personal information in the classroom. Such risks include significant data breaches, student profiling, biometric surveillance, and manipulative design.

The joint resolution affirms that the right to education and the right to privacy are fundamental and interdependent rights. It calls on governments to assume their responsibility for ensuring student privacy when assessing or authorizing EdTech; education institutions to protect privacy throughout the procurement process; and vendors, to design privacy protective tools that take the best interests of children into account.

FROM THE OMBUDSMAN WEBSITE

Taking children's best interests into account when procuring, designing or implementing EdTech means, among other things:

- Embedding privacy by design into products and services;
- Following data-minimization principles;
- Ensuring that safeguards are proportionate to the sensitivity of collected information;
- Avoiding design practices that would influence, manipulate or coerce users into making decisions that go against their privacy interests;
- Building in appropriate access controls and encryption;
- Establishing privacy settings to their most protective level by default;
- Prioritizing privacy protection when selecting educational technologies; and
- Funding and implementing digital education and privacy training and digital literacy skill development.

FROM THE OMBUDSMAN LETTER TO US

- Delivering and participating in digital education and privacy training and digital literacy skill development
- Continuously exercising diligence and privacy protective practices when procuring and using educational technology including the use of privacy impact assessments where appropriate
- Having appropriate retention and deletion policies for personal information collected, and retain only necessary information for only as long as required
- Ensuring products are secure and privacy protective settings are the default
- Engaging and informing children/youth, parents and guardians of personal information collected, used, disclosed and retained in the use of educational technologies and responding to any concerns raised

FROM THE OMBUDSMAN LETTER TO US (GOV'T)

- Reviewing, adapting or amending privacy legislation in the context of emerging and evolving technologies to effectively protect children's privacy rights
- Funding and implementing digital education and privacy training and digital literacy skill development
- Publishing procurement rules for EdTech that demonstrate compliance with legislation and embed the use of privacy assessments when selecting, procuring and reviewing educational technologies

NOTES

NOTES

PowerSchool Incident – Lets Be Practical!

- Failed to include sufficient privacy / security provisions in the agreements with PS to meet provincial law
  - Have you tried to negotiate with a technology vendor?
  - Do we need to insist on provincial law reference if standard otherwise met?
  - MAYBE government needs to procure / set terms?
- Lacked policies / procedures to monitor and oversee PS's security safeguards to ensure compliance with contractual terms (e.g. MFA)
  - This was the ONLY option in the market – how risk assess now / later?
  - Anyone doing this for Microsoft? *How can we review the experts??!!??*
  - Is each Division required to audit / follow up / demand ISO reports?
  - MAYBE government needs to take this on?

PowerSchool Incident – Lets Be Practical!

- We do need to recognize that breach is inevitable BUT NEED DATA!
- SO ….
  - You still need to collect what you have to collect – GOV'T clarify?
    - PHIN (ambulance) / SINs (CRA)
  - Do we purge databases / network drives (student/staff) every few years? ***Like a student locker?***
    - What do we need NOW? (contact info, medical, PHIN, SIN)
    - What do we need LATER? (marks)
  - Do we need to consider placing some things "off-line"?
    - Long term retention of CFS reports? / **ENCRYPTION?**

WHEN A REQUEST COMES IN….

- Time limit for responding is 45 calendar days after receipt (s.11(1)). Can extend for an additional 30 days (s.15)
  - Responding within the time is unreasonable because of the large number of records requested or that need to be searched
  - Time is needed to consult with third party, another public body, or to obtain legal advice
  - Exceptional circumstances warrant the extension
- Consultation is OK – internally, MSBA and lawyer
  - **BUT keep Applicant name secret (unless necessary – e.g. parent)**

THE RECORDS

- Applies to ALL records = Default position – **DIVISION EMAILS!!!**
- Really only in-camera and privilege left alone – but have to SHOW
  - May need to show excerpts of record / email to prove
  - Personal Information definition includes *the individual's own personal views or opinions, except if they are about another person* and *the views or opinions expressed about the individual by another person*
- Personal emails versus **work emails**
  - **CUSTODY AND CONTROL** issue → mandate / function of Division?
  - All Division controlled emails – on face - subject to FIPPA
  - *May need to keep on hand if litigation risk / demand to preserve records*

THE RECORDS

- No obligation to create records (unless otherwise required)
- Consider summarizing data versus providing records
  - s.10(2) - public body may create record in the form requested if simpler or less costly
  - s.14(2) - you can give the applicant any additional information to explain the record – designed to explain “government speak”
- Organized response is a sign of good faith
- You can provide further context / information / data
  - Bullying Canada Example

THE SEARCH

- Entitled to charge a search and preparation fee if search and preparation will take more than two hours
  - Regulation says the fee payable is $15 for each half hour in excess of two hours
  - Cannot charge fees for redaction

THE RESPONSE…

- **TRY NOT TO JUST PARROT THE LEGISLATION -**
- Contents of Response (s.12)
  - If record does not exist or cannot be locate, state this. You may be asked by Ombudsman to explain efforts to locate (including asking key people)
  - If access is refused for record that exists and can be located, need to list:
    - the reasons for the refusal
    - the specific provision of FIPPA on which the refusal is based
    - title and contact information of an officer/employee who can answer questions
    - that the applicant may make a complaint to the Ombudsman
- Can disregard certain requests (s.13)
  - Trivial, frivolous, vexatious
  - Unduly repetitive, broad, or incomprehensible, not made in good faith
  - Unreasonably interfere with the operations of the public body

EXCEPTIONS TO DISCLOSURE

- Withholding of record versus redactions
- Section 7(2) – redact until it is no longer reasonable
  - The right of access does not extend to information that is excepted from disclosure. If information can reasonably be severed, applicant has right of access to remainder of record.
- Proper redaction
  - Emails – "Good morning", dates, "have a great weekend", *business email addresses* → all included
  - Good example – emails sent to Division (need to sufficiently redact so people cannot be identified – local knowledge?)
- **If discretionary – consider whether want to redact?**
- Yellow / Black / **IRREVERSIBLE** REDACTION!!

EXCEPTIONS TO DISCLOSURE

- Section 17 – Privacy of a Third Party
- **(1) MUST refuse disclosure of personal information if disclosure would be an unreasonable invasion of third party's privacy**
- 17(2) Disclosures deemed to be an unreasonable invasion of privacy
  - (a) personal health information
  - (e) employment/educational history
- There are exceptions in 17(4)
  - (e) the information is about the third party's job classification, salary range, benefits, employment responsibilities or expenses as an officer or employee

Parent email about their child is likely NOT personal information of that parent and, as such, may have to be shared with other parent

EXCEPTIONS TO DISCLOSURE

- 17(3) Determining unreasonable invasion of privacy
  - (a) disclosure is desirable to subject activities of the public body to scrutiny;
  - (b) disclosure is likely to promote public health or safety;
  - (c) disclosure will assist in a fair determination of the applicant's rights;
  - (d) disclosure may unfairly expose the third party to harm;
  - (e) the personal information has been provided, explicitly or implicitly, in confidence;
  - (f) the personal information is highly sensitive;
  - (g) the personal information is likely to be inaccurate or unreliable;
  - (h) disclosure may unfairly damage the reputation of any person referred to in the record;
  - (i) the disclosure would be inconsistent with the purpose for which the personal information was obtained.

EXCEPTIONS TO DISCLOSURE

- Section 18 – Business Interests of Third Party
- MUST refuse disclosure of information that would reveal
  - (a) trade secret of third party
  - (b) commercial, financial, labour relations, scientific or technical information supplied by a third party, explicitly or implicitly, on a confidential basis and treated consistently as confidential; or
  - (c) commercial, financial, labour relations, scientific or technical information the disclosure of which could reasonably be expected to;
    - (i) harm the competitive position of a third party,
    - (ii) interfere with contractual or other negotiations of a third party,
    - (iii) result in significant financial loss or gain to a third party,
    - (iv) result in similar information no longer being supplied to the public body
    - (v) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

THIRD PARTY INTERVENTION

- Section 33 –Third party can consent to disclosure if public body is considering giving access under s.17 or 18,
- MUST give notice to third party and invite them to make representations why information should NOT be disclosed
- If they disagree, and you want to disclose, they can make complaint with Ombudsman BEFORE you disclose
- Be aware of procedure and timelines

EXCEPTIONS TO DISCLOSURE

- **Section 22 – Local Public Body Confidences**
- (1) May refuse to disclose information if disclosure could reasonably be expected to reveal:
  - (a) a draft of a resolution, by-law or other legal instrument; or
  - (b) the substance of deliberations of a meeting of its elected officials or of its governing body or a committee of its elected officials or governing body, if an enactment or a resolution, by-law or other legal instrument by which the local public body acts authorizes the holding of that meeting in the absence of the public
- (2) does not apply if (a) has been in considered in meeting open to public or (b) record is more than 20 years old
- In-camera meetings *Public Schools Act* (s.30(4)) – or intended for

EXCEPTIONS TO DISCLOSURE

- Section 23 – Advice to a Local Public Body - **DRAFTS**
- **(1)** MAY refuse disclosure if disclosure could reasonably be expected to reveal:
  - (a) advice, opinions, proposals, recommendations, analyses or policy options;
  - (b) consultations or deliberations involving officers or employees;
  - (c) positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations;
  - (d) plans relating to the management of personnel or the administration of the public body that have not yet been implemented;
  - …
  - (f) information which could reasonably be expected to result in disclosure of a pending policy or budgetary decision.
- Watch exceptions in (2)
  - (b) Instructions or guidelines issued to officers or employees
  - (h) final report or final audit on the performance or efficiency of the public body, except report of appraisal of performance of individual

NOTES

NOTES

TIPS FROM THE TRENCHES

- Some individuals do repetitive email blasts to staff / trustees
  - Consider formally responding once and then make clear no further response
  - But keep the additional emails somewhere safe! (Transcribe VMs?)
- Some individuals send inappropriate emails which cause stress
  - Set up inbox rules (even if on personal device) delete/file
- While it is not illegal for someone to record a conversation – employees cannot be compelled to be recorded → state this / insist on written communications

FillmoreRiley

TIPS FROM THE TRENCHES

- FIPPA of your video surveillance
  - Do we need to consider SHORTER retention period?
    - Works for the subpoena risk as well!
  - Do we need to consider less video recording?
    - Scary principal stare instead?
  - Assert redaction not possible given others in video / **$$**?
  - Assert 17(3)(i) – disclosure inconsistent with purpose for which PI was collected (clear policies) → **function creep**
    - Is for security of property and person / not discipline or performance (and not used for such)
      - We don't let parents re-interview the teacher / staff …
    - "Major penalty" to use a hockey analogy?
  - Who gets to look at it? Avoid audio? MTS position?
  - Consider Ombudsman Guidance Document

FillmoreRiley

FEEL FREE TO CONTACT US

Paul K. Grower
Fillmore Riley LLP
1700 - 360 Main Street
Winnipeg, Manitoba
R3C 3Z3

Telephone: (204) 957-8369
Facsimile: (204) 954-0369
E-Mail: pgrower@fillmoreriley.com

FillmoreRiley