Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MC18-17

Halton District School Board

February 7, 2022

Summary: The Office of the Information and Privacy Commissioner of Ontario (the IPC) received a privacy complaint from the parents of students of the Halton District School Board (the board), objecting to the board's use of third party apps ("apps"), and the associated collection, use, and disclosure of students' personal information. The complainant alleged that the board's utilization of these apps contravened the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA* or the *Act*). The complainants' concerns included a failure to regulate the third party apps available to students via the board's platform, a failure to track which apps had collected students' personal information and what information they had collected, the posting of students' personal information without knowledge or consent, and third party apps advertising to students. The complainants also stated that the board does not have reasonable measures in place to ensure that third party vendors protect the security of student personal information.

This report concludes that the board's catalogue system regulating the apps that collect, use, and disclose students' personal information is in partial compliance with the *Act*, but that the board's notice of collection was deficient. This report concludes that personal information was used for advertising or marketing purposes, contrary to the provisions of the *Act*. This report recommends that the board review its usage agreements with vendors, and revise the agreements to expressly prohibit the use of personal information by vendors for advertising or marketing purposes and to ensure that vendors only use personal information for the board's education-related purposes. This report further recommends that the board review which apps use personal information for marketing or advertising purposes, and take the steps needed to prevent vendors from using personal information for those purposes going forward.

This report also concludes that the board does not have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students. This report recommends that the board revise its usage agreement to require vendors to notify

the board when they have been compelled by law to disclose personal information. This report further recommends that the board revise its usage agreement to include both a requirement that vendors delete data for accounts no longer in use and a commitment by vendors to confirm, on the board's request, that this deletion had occurred. Finally, this report recommends that the board's usage agreement include both an audit requirement and a term stating that vendors' obligations regarding personal information continue to apply, regardless of any changes to a vendor's business name, structure, or ownership.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990; R.R.O. 1990, Regulation 823; *Education Act*, R.S.O. 1990.

Orders and Investigation Reports Considered: Privacy Complaint Reports MC16-10 and PR16-40.

Cases Considered: *Cash Converters Canada Inc. v. Oshawa*, 2007 ONCA 502.

OVERVIEW:

[1] The Office of the Information and Privacy Commissioner of Ontario (the IPC) received a privacy complaint under the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA* or the *Act*) relating to the collection, use and disclosure of personal information by the Halton District School Board (HDSB or the board).

[2] The complainants are parents of two children who were enrolled in HDSB elementary schools at the time. They assert that the board is disclosing students' personal information to online service providers without consent and in contravention of the *Act*. The complainants' concerns include the use, disclosure, security and retention of students' personal information that third party vendors are able to access in providing services to the board.

[3] The complainants raise concerns that third party apps, extensions and add-ons are available to students via the school's G Suite Marketplace platform. Students may download these independently or be directed to do so by teachers. In some cases, the board sets up accounts for the students with third party vendors. The complainants state that through this platform, students were able to access and download third party apps, extensions and add-ons freely and unmonitored. They state that when students access these apps, the apps collect excessive amounts of personal information from these students.

[4] The complainants state that the board does not have a full picture of what accounts students may have registered for via their board emails, or the personal information vendors may have access to as a result. They also allege that the board was not able to provide the complainants with an account of all the vendors who had their children's personal information via accounts registered using board email addresses.

[5] According to the complainants, their children had accounts registered with third

party vendors, without their knowledge or consent, and allege the board provided those vendors with their children's first names and board email addresses. They believe that the existence of these accounts may compromise their children's safety, security, and privacy.

[6] The complainants also claim that students were able to use their board emails to register for services contrary to the terms of service of those tools. They offer the example of tools intended for users over the age of 13 being used by students under that age, without the consent of their parents.

[7] The complainants state that one of the vendors also had their daughter's photo, name and email, and that the content created by his child was viewable on the vendor's public website. The complainants also advise that their child received advertising and marketing emails from some vendors.

BACKGROUND:

[8] The board is an English language public school board that provides education services and education-related services to approximately 65,000 English public elementary and secondary students who reside in the Halton region and attend 93 different schools.

[9] The board has an agreement, including an addendum, with Google to provide core online educational services that are used by its students and teachers, collectively called G Suite for Education Services (G Suite)[1]. Both the agreement and the addendum were negotiated by the Ontario Ministry of Education, for use by school boards within the province. Google also provides additional services to the board, including YouTube.

[10] The board utilizes other online tools in the course of its students' education. These are provided by third party vendors and can be accessed via a vendor's website or application. The board provides a G Suite Marketplace from which students may access tools. The board determines which tools are available in that marketplace and provides guidance to teachers as to how they may be used. The board also sets up accounts for students for some tools and students may individually set up accounts for other tools.

ISSUES:

[11] The following issues were identified as arising from this investigation:

1. Does the information at issue qualify as "personal information" under section 2(1) of the *Act*?

[1] This service is now offered by Google under the name Google Workspace for Education Fundamentals.

2. Was the board's collection of the information at issue in accordance with section 28 of the *Act*?

3. Did the board provide a notice of collection as required under section 29(2) of the *Act*?

4. Was the board's use of the information at issue in accordance with section 31 of the *Act*?

5. Was the board's disclosure of the information at issue in accordance with section 32 of the *Act*?

6. Does the board have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students, in accordance with the requirements of the *Act* and its regulations?

RESULTS OF INVESTIGATION:

Issue 1: Does the information at issue qualify as "personal information" under section 2(1) of the *Act*?

[12] Section 2(1) of the *Act* states, in part:

> Personal information means recorded information about an identifiable individual, including,
>
> > (a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.
> >
> > (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
> >
> > (c) any identifying number, symbol or other particular assigned to the individual,
> >
> > (d) the address, telephone number, fingerprints or blood type of the individual,
> >
> > (e) the personal opinions or views of the individual except if they relate to another individual,
> >
> > (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies

> to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and
>
> (h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

[13] The list of examples of personal information under section 2(1) is not exhaustive. Therefore, information that does not fall under paragraphs (a) to (h) may still qualify as personal information.[2]

[14] To qualify as personal information, the information must be about the individual in a personal capacity and it must be reasonable to expect that an individual may be identified if the information is disclosed.[3]

[15] The issues the complainants have raised encompass a number of different apps or tools. These tools perform different functions and require different student information. The result is that there is a broad array of information at issue, not all of which is at issue for each tool. This includes a student's: full name, student number, Ontario Education Number (OEN), grade level, location, email, password, classes, parent's/guardian's email address, performance data, date of birth, enrolment dates, individualized education plan indicator, and photos.

[16] In addition, some of the third-party tools are used to produce or transmit students' work products such as evaluations, essays, and assignments.

[17] In my view, the information described in the paragraphs above meets the requirements of one or more of the subsections set out under the definition of "personal information" in section 2(1). I therefore find the information at issue is "personal information" as described in the *Act*.

Issue 2: Was the board's collection of the information at issue in accordance with section 28 of the *Act*?

The Complainants' Representations:

[18] The complainants believe that Google and other third party vendors are collecting more of the students' personal information than is necessary, contrary to section 28(2) of the *Act*. The complainants state that some tools are themselves unnecessary to the

---

[2] Order 11.
[3] Order PO-1880, upheld on judicial review in *Ontario* (*Attorney General*) *v. Pascoe*, [2002] O.J. No. 4300 (C.A.).

education of students, and that others, even if necessary, collect more personal information than is needed for the tools to function.

[19] The complainants further state that their children's personal information was obtained by the third party vendors without their parental consent, or the consent of their children. The complainants noted that this is contrary to the terms of service of some of these tools, which require the consent of the user, or parental consent for users below a certain age.

[20] It is important to note that the complainants have chosen not to have their names or the names of their children disclosed to the board, as is their option under the process of our office. This means that I have not been able to communicate specific allegations of unauthorized collections, uses, or disclosures of their children's personal information to the board, so that the board may investigate and address those specific instances. The board has been provided only with the allegations that do not identify the complainants. The complainants have asked whether the outcome of this report would have been different had they not chosen to remain anonymous. Given the significant passage of time since the complainants' specific allegations that predate the board's current information practices, and the inability of the board to respond to those past allegations without knowing the students' identities, I am not able to speculate how those specific allegations would have been addressed.

[21] In any event, the complainants' allegations are not limited to the specific instances where they allege improper collection, use, or disclosure of their children's personal information. They encompass the board's general approach to the use of tools provided by third party vendors that affect all students. Given the Commissioner's authority to receive representations from the public concerning the operations of the *Act* and to report publicly on broad systemic matters of compliance, this report will focus on the current system the board has in place more generally with respect to the collection, use, and disclosure of personal information associated with these tools and make recommendations that are forward-looking.

The Board's Representations:

[22] At the outset, the board states that it is not required to obtain consent for the collection of personal information if it is necessary to the proper administration of a lawfully authorized activity. The board's position is that parental consent is not required for a student to use a particular tool unless the board and the third party vendor explicitly agree that consent from parents will be sought prior to use.

[23] The board advises that it collects the personal information of students and parents in relation to online educational services pursuant to section 28(2) of the *Act*.

[24] The board states that the online educational services provided are for lawfully authorized activities identified in legislation and regulations, Ministry of Education policies and guidelines, and the direction provided by the elected Board of Trustees of the HDSB.

[25] The board advises that the collection of personal information through online educational services is for the purpose of providing education and education-related services such as instruction, assessment, and evaluation for educational programming, as well as for ancillary and administrative services to support the provision of instruction, assessment, and evaluation services.

[26] The board collects this information in different ways at different times. The board collects some of the personal information regarding students and their guardians via its registration form. The board states this is necessary in order to verify the attendance and participation of students as required under section 21 of the *Education Act*. The registration form addresses collection of personal information, stating that "it will be used for purposes related to the regular operational requirements of the educational and administrative functions of the Halton District School Board."

[27] In addition, teachers also regularly collect information on behalf of the board when students produce work. This work product reflects the students' knowledge, learning skills, work habits, behaviour, learning style, learning strengths and weaknesses, engagement, achievement of educational program expectations and opinions. The board uses this information to facilitate providing its services.

[28] The board advises that its collection of personal information in the form of work product is necessary for the board to provide services, including instruction, assessment and evaluation of students pursuant to section 169.1, 170(1) and 171(1) of the *Education Act*.

[29] The board also states that the institution, not the individual receiving services, determines the necessity of the personal information being collected. In other words, it is the responsibility of the board's administrative and teaching staff to identify the personal information necessary to fulfill its duties to students pursuant to the *Education Act*. It is not the responsibility of the student or the parent to determine the personal information required.

[30] The board notes that it collects some work product that is generated by students when they interact with tools provided by third party vendors. The board characterizes this as an indirect collection, and states that such collection is authorized pursuant to section 29(1)(b) and 32(d) of the *Act*. The board advises that this collection is necessary to provide services authorized under section 169.1, 170(1) and 171(1) of the *Education Act*, and which are contemplated under the Ministry of Education guidelines titled *Growing Success* and *Learning for All* and the board's strategic plan.

[31] Regarding the complainants' statements that the board did not obtain parents' consent for vendors to collect their children's personal information, the board's position is that these third parties collect this information on the board's behalf, and that consent is not required when the collection is necessary to provide educational services. The board further states that in cases where a parent objects to collection, the board is not required to offer alternative services that do not involve the collection of personal information.

[32] The board advises that vendors collect aggregated and/or anonymized student information in order to provide the contracted services effectively and to make improvements to the services. The board advises that information collected for these purposes is not personal information because it is not about an identifiable individual.

Analysis

The Catalogue System

[33] Since the time that the complainants initially contacted this office with their concerns about apps and other tools being easily accessed by students, the board has implemented a catalogue system, which permits students to access only approved tools from third party vendors.

[34] This system provides guidance to teachers on tools that the board has centrally reviewed. The board notes that these tools are centrally regulated when they are being accessed on the HDSB.ca network domain, but that students are not prohibited from using their board-issued email accounts when signing up for and using digital tools on other network domains.

[35] The board uses a "stoplight" system, where tools are divided into three categories: red, yellow, and green. According to the board's guidance, red tools should not be used, and the board will identify alternatives. Red tools are not to be installed on board devices and are not available from the board's Google Marketplace.

[36] In contrast, both yellow and green tools are installed and supported by the board, and are available from Google Marketplace. Green tools can be used without concern. The board states that "yellow tools may be used with caution and appropriate professional judgement."[4] Yellow tools have accompanying usage notes for teachers to review and follow in their use.

[37] As of September 2019, the board has restricted the tools available in the board's Google Marketplace to those that the board has either procured, or reviewed and centrally approved. The board states that those tools that collect personal information "are subject to contractual terms that prohibit ownership of student personal information and restrict disclosure of student personal information." Based on the information provided by the board, these restrictions are set out in written agreements. These agreements can be either what the board calls a "Non Disclosure Agreement" (the Usage Agreement) or an individualized contractual arrangement between the board and the vendor.

[38] Among the characteristics that determine how each tool is categorized, is the extent of personal information that is being collected. The board states that apps that collect personal information beyond what is needed for the function of the application are

[4] HDSB guidance document "Criteria and Considerations for Privacy Reviews."

classified as red. Yellow tools should not use or store student information, or if they do so, the data should be anonymized. Green tools either do not use personal information, or when they do, they should "have the full benefit of appropriate technical, physical and administrative controls and reflect a lawfully authorized use of Personal Information".[5]

Relevant Tools

[39] The complainants flagged a number of tools and set out concerns they had with the collection, use, and/or disclosure of personal information by the third party vendors of those tools. These include:

- G Suite for Education and YouTube, operated by Google;
- Raz-Kids, operated by Learning A-Z;
- Dreambox Learning;
- Duolingo;
- Mathify operated by TV Ontario;
- Brightspace operated by D2L;
- All About Me and myBlueprint Education Planner, operated by myBlueprint;
- School Cash Online operated by KEV Group;
- WeVideo; and
- Infogram.

[40] The board provided this office with a summary of its analysis of the personal information collected by, used by, and disclosed to the tools listed above, as well as their contractual relationship, if any. The list of tools noted above includes tools that fall into either the yellow or green categories of use.

[41] The complainants' overall contention is that the system that the board has in place to protect its students' personal information is inadequate, and that the board does not have adequate controls in place to know what information those vendors have access to or have sufficient guardrails on that information. The complainants provide some specific examples of collections, uses, and disclosures that they state demonstrate these inadequacies.

[42] It is clear that the complainants' larger issue is with the system that the board has put in place to protect students' personal information. In their initial complaint, they

---

[5] Ibid.

stated that the system was essentially non-existent, and they still view the system put in place since as inadequate. Given this, instead of evaluating each tool, I will be focusing on whether the catalogue system establishes adequate protections to ensure that personal information is only collected, used, and disclosed by vendors in compliance with the *Act*. If the system adequately ensures that a tool is only collecting the personal information necessary for its use for educational purposes, there is no need for the IPC to make a determination on each tool in use under that system.

[43] I also want to address the complainants' comments regarding lack of consent for the collection of their children's personal information. The complainants seem to take the position that a third party cannot collect students' personal information, even on behalf of the board, without the consent of the parents or guardians.

[44] The board describes the vendors as indirectly collecting personal information, and states that the vendors are permitted to do so under section 29(1)(b) of the *Act*. Section 29(1) states that institutions "shall collect personal information only directly from the individual to whom the information relates" unless an exception set out in subparagraphs (a) to (h) applies.

[45] The exceptions set out at section 29(1) list the circumstances in which indirect collection is permitted vis a vis the institution, relative to its agent. It does not, however, assist the board in authorizing collection of personal information from the students or parents in the first place, whether acting on behalf of itself or through an agent.

[46] In any event, the board states that consent is not necessary, as it cites section 28(2) of the *Act* as authority for its collection of students' personal information.

[47] This section of the *Act* sets out the circumstances under which personal information may be collected by or on behalf of an institution. In order for such a collection to be permissible under the *Act*, it must satisfy one of the following conditions: it must either be (1) authorized by statute; (2) used for the purposes of law enforcement; or (3) necessary to the proper administration of a lawfully authorized activity.

[48] In this investigation, the collection of personal information in question is not expressly authorized by statute, and the information is not being used for the purposes of law enforcement. Accordingly, in order for the collection of personal information to be permissible under the *Act*, it must be shown to be necessary to the proper administration of a lawfully authorized activity.

[49] The test for determining whether a collection of personal information is necessary to the proper administration of a lawfully authorized activity was enunciated by the Ontario Court of Appeal in *Cash Converters Canada Inc. v. Oshawa*[6] as follows:

---

[6] 2007 ONCA 502.

> the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the Act.

[50] I refer to the requirement set out above as the "necessity test." In order to satisfy this condition, an institution must identify the lawfully authorized activity in question, and then explain how the collection of personal information is necessary to its administration.

[51] The board states that it collects personal information for the purpose of providing education to students. This includes instruction, assessment, and evaluation for educational programming as well as supporting ancillary and administrative services. The board states that these services are lawfully authorized activities identified in legislation and regulations, as well as in Ministry of Education guidance. In particular, the board cites sections 169.1, 170(1), 171(1), 264(1) and 265(1) of the *Education Act* as authority to provide education related services. I agree that the provision of education and education-related services to students is a lawfully authorized activity.

Are the tools necessary?

[52] The complainants have alleged that individual collections of personal information are unnecessary and that the use of several of the tools themselves are unnecessary for students' education. Two of the tools that the complainants single out as unnecessary are Duolingo and RazKids.

[53] The board acknowledges that its collection of personal information is limited by the necessity requirement set out in section 28(2) of the *Act*. However, it states that it is the institution's role to evaluate whether the collection of personal information is necessary to the proper administration of a lawfully authorized activity.

[54] Necessity is one of the matters the board considers in its guidelines for reviewing software for the catalogue system. In those guidelines, the board states that if a tool does not support the board's needs, it will be categorized as red, and not be used. This is the first step in reviewing any tool.

[55] The board is the institution responsible for providing educational services, and is in the best position to determine the tools it requires to do so. I agree with the board that whether a *tool* is necessary for the provision of educational services is a matter for the board to decide. However, this leaves open the question of whether the *personal information* that is collected by the tool is necessary to the provision of educational services.

The Catalogue System – Collection Protections

[56] The complainants claim that regardless of the school board's need to use the tools

themselves, some of these tools collect more personal information than is required.

[57] The board has established a system to address this. It has set up a catalogue system where it determines which tools students can access without restriction and which can be used with restrictions in place. One of the requirements of that system is that the tool only collects the personal information required for the functionality of the tool.

[58] In its catalogue guidelines, the board states that over-collection of personal information is a characteristic that would lead to the board categorizing the tool as red. These guidelines provide examples of collection beyond what is needed for the application to function, such as being granted access to Google Drive or tracking user activity.

[59] The board provided assessments for the tools raised by the complainants in their submissions. These assessments consider factors including the personal information collected by the board via the vendor, the personal information collected by the vendor, and any other information collected.

[60] Among these are assessments for RazKids and Duolingo, two tools that the complainants state were collecting more information from students than required. I will review the board's assessments for these tools, as a means of determining whether the board's categorization system adequately addresses whether a tool only collects personal information that is necessary for it to function.

[61] RazKids is a green tool that the board states provides "personalized reading instruction, assessment and practice for K-6 classrooms, leveled reading resources, teacher resources, quizzes." Teacher, student, and parent portals are available within this service. The board collects assessment and communication information, while the vendor collects the student's first and last name, classroom roster, and OEN, as well as the parent's email address.

[62] The board states that the personal information collected by the various tools is necessary to the provision of educational services. I accept that a tool providing reading instruction would need to provide assessments to the school board, as well as a means of communication between the board and students. Similarly, I am satisfied that such a tool would require a student's name, classroom roster, OEN, and a parent's email address for its use to perform these functions.

[63] Duolingo is a yellow tool, which the board describes as "gamification to support French language learning." In contrast to RazKids, students do not create accounts to use Duolingo, so no identifiable information is provided to the vendor. Instead, teachers may choose to use this tool such that any collection of student information is limited to their assessment or engagement in a non-identifiable form. The vendor also collects device information, mobile network information, log information, location information, application numbers, and cookies. However, the board states that because Duolingo is only used on board devices, the board itself is identified but not the individual user.

[64] The foregoing shows that because the use of Duolingo does not require individual students to set up accounts, Duolingo does not collect identifying personal information from the students using the tool.

[65] As noted above, I have reviewed the RazKids and Duolingo examples to assess the board's catalogue system, and its ability to determine whether a tool collects more information than necessary. The catalogue system uses over-collection as a criterion in determining whether a tool will be categorized as green and permitted to collect students' personal information. I am satisfied that this system satisfies the board's obligation to ensure that it collects, directly or through its agents, only the personal information necessary for the provision of educational services. I find that the collection of personal information permitted under this system is authorized pursuant to section 28.

Issue 3: Did the board provide a notice of collection to parents as required under section 29(2) of the *Act*?

[66] Under the *Act,* an institution is required to provide individuals with formal notice of the collection of their personal information. The purposes of the notice are to ensure that an institution's practices with respect to personal information are transparent and that an institution is accountable to the individual. In addition, the notice of collection may serve to reduce any concerns regarding the collection and use of personal information.[7]

[67] Section 29(2) of the *Act* imposes a notice requirement on institutions that collect personal information. Section 29(2) states the following:

> (2) If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,
>
> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

[68] Accordingly, under the *Act,* the board is required to provide individuals who are subject to a collection with a Notice of Collection containing the elements listed above.

Complainants' Position:

[69] The complainants argue that the board does not provide students and parents with

---

[7] PC12-39, page 10.

proper notice as required by the *Act*.

[70] The complainants advise that the "Statement of Personal Information Practices" (the Statement) posted on the board's website is inadequate and unclear regarding the purposes for which the board collects, uses, and discloses personal information. They also state that they received conflicting information from the board as to whether teachers were responsible for advising parents about the use of G Suite services.

Board's Position on Notice:

[71] The board advises that it provides notice two ways. First, at the time of registration, via the notice included as part of the Student Registration Form. Second, via the Statement it provides to students annually which is also available on the board's website. The board notes that it also provides the "Privacy and Information Management Policy" and the "Responsible Use Procedures for Information and Communication Technology" to students during the registration process.

[72] The board states that the notice provided in the Statement applies to Google (as the vendor for G Suite) and the other third party vendors providing tools. The board also notes that individual teachers may bring the use of different tools to the notice of parents and that parents are encouraged to discuss instructional methods in use with their children's teachers.

Analysis:

[73] Section 29(2) of the *Act* requires that a notice of collection include three pieces of information: the authority for the collection; the principal purpose for which the information is to be used; and contact information for an agent who can answer questions about the collection.

[74] The board points to two notices of collection found in the Student Registration Form and the Statement. The notice in the Student Registration Form also refers readers to the Statement for more information. I will first address the notice provided in the Statement.

[75] While the board provided the IPC with a 2017-2018 copy of the Statement, this has since been updated. I will address the most current version available online, applicable to the 2020-2021 school year.

[76] In that Statement, the board cites legislation for its authority to collect personal information, including *MFIPPA* and the *Education Act*. It includes the following paragraph regarding personal information:

> Routine uses of personal information:
>
> The HDSB collects, uses and discloses personal information about students, parents/guardians and other parties in accordance with the law and for

> purposes related to the provision of education and ancillary services. The authority for the collection, use and disclosure of personal information is derived from the Education Act. The process for collection, use and disclosure is identified in MFIPPA. For additional information regarding the HDSB's practices related to Information Technology please refer to the Board's Technology and You page (visit www.hdsb.ca and search "Technology & You").

[77] The "Technology & You" page linked in the Statement addresses Digital Learning Tools generally, as well as G Suite, Brightspace, and myBlueprint specifically. The Digital Learning Tools section states:

> The Halton District School Board is committed to delivering digital learning opportunities to all students to support global competencies.
>
> All HDSB students and staff have a G Suite and email account. Students in K-12 will not be able to use their Halton Cloud/G Suite account for G-Suite Marketplace, Chrome Web Store or to register for a 3rd party website/application/software unless the software has been approved for education use by HDSB.
>
> Student use of approved applications are available through the HDSB Marketplace and HDSB Chrome Web Store. See G SUITE for additional details.
>
> Students are provided with a variety of digital learning tools including:
>
> G-suite for Education
>
> Brightspace Online Classroom
>
> myBlueprint (6-12)/All About Me (K-5)

[78] The Statement goes on to list the broad purposes for which the board collects, uses, or discloses personal information, including:

- "to assess and evaluate student achievement, create and maintain Ontario Student Records, transcripts and progress reports for each student";
- "to facilitate educational activities via IT partnerships and contracts (e.g., G Suite for Education, SchoolMessenger communication, Library and Student Information systems)"; and,
- "for purposes related to the regular operational requirements of the educational and administrative functions of schools and the school board".

[79] The Statement also includes a passage setting out who may be contacted with

inquiries, stating that "[q]uestions about the information handling practices of the Halton District School Board may be directed to your school Principal or to privacy@hdsb.ca."

[80] Turning to the requirements for a notice of collection, the board has satisfied the section 29(2)(a) requirement by specifying its legal authority to collect students' personal information.

[81] The Statement also addresses the purposes for which the information is intended to be used, stating that it is for "the provision of education and ancillary services." This includes a non-exhaustive list of tools that the board uses in providing those services, illustrating the types of board tools that make use of students' personal information. Additional information on the use of students' personal information is also found on the linked "Technology & You" page. I find that the board has satisfied the section 29(2)(b) requirement that a notice of collection include the principal purposes for the use of personal information.

[82] The third requirement is that the notice include "the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection." The Statement refers readers to either their principal, or to a general email address. It does not include any of the required employee title, address, or telephone number. The notice included in the Student Registration form likewise does not include this information. Accordingly, I find that the notice as currently published on the board's website is not in accordance with section 29(2)(c) of the *Act*.

[83] I recommend that the board revise the current notice in the Statement to include the title, business address, and business telephone number of an officer or employee of the board who can answer questions regarding the collection of personal information.

Issue 4: Was the board's use of the information at issue in accordance with section 31 of the *Act*?

[84] Section 31 of the *Act* states:

> An institution shall not use personal information in its custody or under its control except,
>
> > (a) if the person to whom the information relates has identified that information in particular and consented to its use;
> >
> > (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
> >
> > (c) for a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the *Freedom of Information and Protection of Privacy Act*.

[85] Section 33 defines consistent purpose as referenced in section 31(b) as follows:

> The purpose of a use or disclosure of personal information that has been collected directly from the individual to whom the information relates is a consistent purpose under clauses 31(b) and 32(c) only if the individual might reasonably have expected such a use or disclosure.

Complainants' Position:

[86] The complainants note that since bringing this complaint to the IPC, the board has changed its approach to the use of third party apps, and now requires usage agreements to be in place before it allows students to use those tools. The complainants state that prior to 2019, the third party apps were not restricted in such a way. The students themselves accepted the terms of service, and the complainants allege that the board did not have a full account of where student information had gone, or for what purpose it had been used.

[87] The complainants also note specific concerns regarding uses of their children's personal information prior to the board putting its catalogue system into place. These include their child's personal information being posted publicly without their knowledge and vendors sending their child advertising and marketing emails.

[88] The complainants state that vendors did not use students' personal information for the same purpose for which it was originally compiled and that such use was not necessary for the education of the student or for the administration of an education program.

Board's Position:

[89] The board states that it uses the personal information of students and parents for the purpose of providing education and education-related services. Such services include instruction, assessment, and evaluation for educational programming as well as ancillary and administrative services to support the provision of instruction, assessment, and evaluation services. The board states that these services are provided as part of its authorized activities identified in legislation and regulations, Ministry of Education policies, guidelines and the direction provided by the elected Board of Trustees of the board.

[90] The board's position is that all of these uses of personal information are for the purpose for which the personal information was compiled or for a consistent purpose. The board states that the purpose for which the personal information is being used has a reasonable and direct connection with the board's duties and responsibilities to provide publicly funded services.

[91] The board states that when determining whether the board's use or disclosure of personal information is for a purpose consistent with its collection, the test is whether the individual "might reasonably have expected such a use or disclosure." The board states

that the Statement provides examples of when, how and why personal information may be collected, used and disclosed by the board. The board's position is that an individual's reasonable expectations regarding use of personal information should be assessed in the context of the information the board has communicated about these services.

[92] The board advises that the products and tools provided by the vendors and used by the board are necessary for the board to meet the expectations identified in its strategic plan; to provide evidence-based instructional strategies, resources and interventions that are differentiated to students learning needs; and to support data informed decision making regarding student programming.

[93] The board also notes that as of September 2019, board students would not be able to connect their board G Suite account with third party web-based tools and apps unless there is a contract in place between the vendor and the board that addresses disclosure of students' personal information. More recently, in a letter to the IPC, the board confirmed that those restrictions had been put in place, stating as follows:

> Beginning in September 2019, the HDSB began restricting the Apps available in the HDSB G-Suite Marketplace for use with students to only those Apps procured and/or reviewed and approved centrally by the HDSB. Apps made available in the HDSB G-Suite Marketplace, which collect personal information, are subject to contractual terms that prohibit ownership of student personal information and restrict disclosure of student personal information.

[94] Though the above statement only refers to disclosure, the contractual terms in the Usage Agreement also include restrictions on use of personal information.

[95] The board advises that these restrictions assist the board in monitoring the personal information accessible by these tools and apps.

Analysis

[96] As with the analysis of the collection of personal information, I will examine the board's system, so that I can evaluate whether it has adequate protections in place for how a vendor may use students' personal information.

[97] Broadly speaking, the complainants are concerned about how some tools obtained their children's information, what they are doing with that information, and what the board is doing to ensure that their children's personal information is not being used improperly.

[98] Section 31(b) of the Act states that "an institution shall not use personal information in its custody or under its control except … for the purpose for which it was obtained or compiled or for a consistent purpose."

[99] I have already addressed the collection of personal information by and on behalf of the board, under the catalogue system, as well as the purpose of this collection. I found that this system limited the personal information collected to that necessary for the proper administration of a lawfully authorized activity, namely the provision of educational services pursuant to the *Education Act*.

[100] This catalogue system addresses both prohibited and permitted uses of personal information. The board's description of "What a Red Tool Looks Like" includes characteristics of tools that would not be permitted to access personal information. These include vendor tools capturing analytics of user behaviour when that data is not aggregated or otherwise anonymized, and "[collection/use/disclosure of] user personal information for commercial purposes or non-educational reasons either by making it public or via third party partnerships."[8] This description indicates that tools in which the vendor uses personal information for its own purposes, rather than board purposes, would not be permitted for use by students or teachers.

[101] The board states that vendors are acting on the board's behalf when using personal information and that the board engages vendors to use this personal information for the board's purposes, not the vendors' purposes. This is consistent with paragraphs 5 and 6 of the board's Usage Agreement:

> 5. The Vendor agrees that the Personal Information of students and/or parents/guardians [or employees] may only be collected, used, retained and disclosed by the Vendor for the purpose of fulfilling its contractual obligations to the Board.
>
> 6. The Vendor agrees that any Personal Information collected, used, retained and/or disclosed by the Vendor during the course of providing goods/services for the Board shall remain under the control and direction of the Board for the sole purpose of providing goods/services for the Board and for no other purpose. The Vendor shall not collect, access, use, retain, disclose, sell or share Personal Information for its own benefit or purpose.

[102] Not every vendor executes the board's standard Usage Agreement; some sign modified versions of the Usage Agreement, or individualized contracts. However, based on the contracts provided to the IPC, vendors of tools permitted to access student personal information provide largely equivalent protections (with one identified exception, addressed separately below).

[103] For example, the Addendum to Google's G-Suite for Education Agreement limits use as follows:

---

[8] HDSB Guidelines, "Criteria and Considerations for Privacy Reviews."

> Google will use Customer Data for the following purposes: (a) to provide the Services, (b) to operate, maintain, enhance and support the infrastructure used to provide the Services and (c) to comply with Customer's or End Users' instruction in the use, management and administration of the Services; (d) to respond to customer support requests. Google will only use Customer Data in accordance with this Agreement.

[104] The exception to these protections is found in the Usage Agreement that the board entered into with KEV Group. While many provisions of the agreements are identical, the KEV Group Agreement is lacking clauses 5 and 6 in the Usage Agreement, as set out above. Instead, the KEV Group Agreement states as follows:

> The Vendor agrees that any Personal Information disclosed by the Board to the Vendor shall remain under the control of the Board and shall remain subject to the Acts.

[105] The Usage Agreement's explicit prohibition that a Vendor shall not "collect, access, disclose, sell or share Personal Information for its own benefit or purpose" provides assurance to the board that personal information that it permits a vendor to access will only be used for the board's benefit. The board's compliance with *MFIPPA* relies on the board restricting any third party vendor's use of personal information. The KEV Group Agreement does not provide adequate assurance that sufficient restrictions on the use of personal information are in place, as it does not close off the KEV Group from using personal information for its own purposes.

[106] The generic Usage Agreement limits uses of personal information to those permitted under the *Act*, but it is not clear that the KEV Group Agreement does so. I was not provided, nor did I request, all the Usage Agreements or similar agreements that the board has in place with vendors of third-party tools. The KEV Group Agreement may be singular but the board may also have other less restrictive agreements in place with other vendors.

[107] Given this, I recommend that the board review all of the agreements that it has in place with vendors of third party tools, identify any agreements that do not provide protections equal to or greater than those found in clauses 5 and 6 of the Usage Agreement, and revise these agreements to provide comparable protections to those clauses.

Posting of Personal Information

[108] The complainants raise other concerns regarding their child's personal information having been made publicly viewable on the internet, without their knowledge. This is information that was linked to the student's account, such that when other information was made publicly viewable, so was this linked personal information. These allegations relate to Infogram, WeVideo, and YouTube, and occurred before the catalogue system was put in place.

[109] As the complainants have filed this complaint anonymously, the board was not given the information necessary to investigate their specific allegations. Furthermore, based on the information provided, I am not able to determine whether personal information was used in contravention of the *Act* in any specific instance in the past. Regarding such uses more generally, however, the board states that Infogram is now permitted for staff use only, and WeVideo use is only permitted with "cautions and specifications" regarding how that tool may be used. Given this, I will not be reviewing the specific allegations regarding Infogram and WeVideo any further.

[110] However, the complainants' allegations regarding YouTube are both clearer and of continuing relevance. The complainants state that their child posted comments on YouTube, and that G Suite auto-filled the name of their child in connection with these comments. This resulted in their child's name being displayed on YouTube comments without the child having entered their name for that purpose.

[111] YouTube allows for anonymous viewing of videos but requires the user to have their own channel in order to comment on videos.[9] YouTube is a service included in G Suite for Education, although it is not one of the Core Services covered by the board's G Suite Agreement. Students accessing YouTube via their G Suite account have their G Suite account information follow them to YouTube. This is visible to students, as they are commenting on YouTube, through the comment field, which states that the user is "commenting publicly as [profile name]". Students also have the option of using a separate YouTube account to post comments if they are concerned about their G Suite profile name being displayed with YouTube comments, and may also choose to leave their G Suite profile photo blank.

[112] The current restrictions on YouTube now limit its use with the board G Suite account to students in ninth grade and above. Given those age restrictions, it is reasonable to expect that students would be aware that commenting on YouTube videos would not be anonymous and would involve their G Suite profile name and profile picture (where one is provided) being displayed with the comment.

[113] I have already determined that the catalogue system adequately ensures that the personal information collected is necessary to the provision of education to students. The question at this stage is not related to necessity, but rather to whether the use is for the purpose for which it was obtained or compiled or for a consistent purpose. In this case, in the circumstances where the board has determined that YouTube is to be used for the purposes of providing education services to students, importing the students' profile information from the Core Services to YouTube is a consistent purpose, and is permitted pursuant to section 31(b) of the *Act*.

---

[9] See YouTube Help, "Post & interact with comments" at https://support.google.com/youtube/answer/6000964.

Advertising and Marketing

[114] The complainants state that their child received direct advertising emails from vendors. From the complainants' submissions, it appears that the vendor at issue in that case was Infogram, which had sent out newsletters and similar emails to the child's board email address.

[115] Screenshots included with the complainants' submissions show a myBlueprint page with chances to enter draws displayed at the bottom of the page. The complainants also provided a screenshot of a WeVideo welcome page that included available plans for purchase.

[116] Due to the anonymity of the complainants, the board was not able to investigate the latter two ads in order to determine if they involved the use of the student's personal information in order to serve the particular ads in question. I will focus therefore on the email marketing because the vendor would necessarily need to use the child's email address in order to send those email ads to them.

[117] In its representations, the board states that vendor privacy statements restricting marketing and advertising are preferred, and may be a consideration of the committee when evaluating software. The board's catalogue system states that apps with advertising or marketing "as part of the terms and conditions and/or sent by email to registered users" are classified as red. However, in its representations the board states that it does not prohibit advertising:

> The Board neither prohibits nor encourages advertising or marketing to students. The Board does not have a policy statement regarding advertising and marketing to students.
>
> The Board respectfully submits that advertising and marketing are not homogenous; there are many different forms of marketing and advertising, both overt and covert. Similarly, what age children and youth should be exposed to marketing and advertising, and what form exposure to advertising and marketing should be permitted, as well as when, where and how much advertising and marketing children and youth should be exposed to are ***not*** opinions that are uniformly held by the parents and guardians of the Board's 65,000 students.
>
> As examples, a vendor might market and/or advertise products or services through contests, surveys and updating information for students who are already using some services offered by the vendor. Very subtle advertising and marketing occur with product placement, which is in contrast to advertisements that might be sent by direct emails.

[118] The board states that each vendor is required to commit to a Student Privacy

Pledge[10], which contains a general prohibition on using "student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student". It also prohibits use of student information for "behavioral targeting of advertisements to students."

[119] The board places undue importance on the Student Privacy Pledge, which is a voluntary commitment that US companies dealing with student data may choose to make. This pledge is an instrument that is enforceable only to the extent that it involves the collection or management of student data by companies operating within the United States in a manner that is contrary to the terms of their public pledge.[11] From the information available on its website, this pledge does not apply to the use of student personal information outside the United States and provides no mechanism for enforcement outside the US. Specifically, this Pledge appears unenforceable as it applies to the HDSB and its students, and there is no indication that a pledge of this nature would provide the same privacy assurances as similar contractual commitments would. The Student Privacy Pledge, therefore, does not protect HDSB students from advertising, behavioural or otherwise. The board has not provided the IPC with any information contradicting this.

[120] The board has not put in place explicit restrictions on vendors prohibiting or controlling the use of students' personal information for advertising. Instead, the board states that advertising or marketing should be at the choice of parents or guardians.

[121] That argument may be relevant to whether the information was used with consent pursuant to section 31(a) of the *Act.* However, in this case, the complainants state that they provided no consent, and the board did not provide evidence showing that the consent requirement was satisfied. Instead, the board has stated that the vendors' use of personal information is authorized under sections 31(b) and 33 of the *Act*. Under those sections, the question to be asked is whether the use was for the provision of educational services or for a consistent purpose.

[122] The IPC has previously found that there must be "a rational connection between the purpose of the collection and the purpose of the use in order to meet the 'reasonable person' tests set out in section 33"[12] and that "a key element of reasonable expectation is foreseeability."[13]

[123] Privacy Complaint Report MC16-10 also dealt with section 33 in the context of

---

[10] Found at https://studentprivacypledge.org/.
[11] The Student Privacy Pledge website addresses enforcement of its commitments, stating that the Federal Trade Commission may "bring civil enforcement actions against companies who do not adhere to their public statements" and thereby engage in unfair or deceptive practices. The website notes that non-American companies that collect or manage data from United States students "are subject to US laws for those business operations and are eligible to take the Pledge." See: https://studentprivacypledge.org/faqs/.
[12] Privacy Complaint Report MCO7-64. See also Privacy Complaint Reports MC16-4 and PC18-18.
[13] Privacy Complaint Report MC16-4.

advertising. In that case, a township provided a warranty company with personal information of residents, so that the company could market their services to those residents. This information had been collected for water billing purposes. This office concluded that a reasonable person would not have expected the use of their personal information to market the warranty program, and that the purpose of the disclosure was inconsistent with the purpose of the collection.

[124] I agree with that reasoning, and apply it in the case at hand. Neither a student nor a parent or guardian would reasonably expect that information they provide to obtain an education would be later used to market goods or services to them.

[125] Students have a reasonable expectation of privacy in the personal information they provide access to in the course of receiving their education. Students, parents, and guardians must rely on the board's expertise to determine the apps that students require for their education. It is reasonable for them to expect the board put in place safeguards to ensure that the information is used only for those purposes.

[126] Indeed, the board itself expects that vendors not use information for their own purposes, as the Usage Agreement states that vendors shall not use personal information for "their own benefit or purpose." Advertising or marketing benefits the vendor, not the board or the students. The presence of that restriction reinforces my conclusion that students would not reasonably expect that their personal information would be used for advertising purposes.

[127] In the present case, the only uses for marketing or advertising that have been established are the marketing emails sent to the student. I find that the student would not reasonably have expected the use of their personal information, as set out in section 33, for advertising or marketing purposes. Accordingly, the use of this personal information by the board's agent was not in accordance with section 31(b) of the *Act*.

[128] This shows that the board's current protections, including the catalogue system and the Usage Agreement (or equivalent agreements), do not sufficiently protect against use of personal information for advertising or marketing purposes.

[129] In order to prevent the unauthorized use of students' personal information, I recommend that the board revise its Usage Agreement (and similar agreements with other vendors) to explicitly prohibit vendor use of students' personal information for marketing or advertising purposes. I further recommend that the board review which apps use personal information for marketing or advertising purposes, and take the steps needed to prevent the vendors from using personal information for those purposes going forward.

Issue 5: Was the board's disclosure of the information at issue in accordance with section 32 of the *Act*?

[130] Under the *Act*, personal information in the custody or under the control of an

institution cannot be disclosed except in the specific circumstances outlined in section 32.

[131] Section 32 of the *Act* states in part:

> An institution shall not disclose personal information in its custody or under its control except,
>
> …
>
> (a) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
>
> (b) for the purpose for which it was obtained or compiled or for a consistent purpose;
>
> (c) if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions;

The complainants' position

[132] The complainants object to the school board setting up accounts for students, and in doing so, disclosing the students' personal information. The complainants believe that the board discloses the student's email address, as well as part or all of the student's name, and possibly the student's location, to third party apps. The complainants cited Infogram, WeVideo, Canva, Powtoon, and Duolingo as examples of tools for which accounts were set up in their children's names.

[133] The complainants state that it is unclear to them who accepts the terms of service and privacy policies of the third party apps when they are downloaded. They believe that many students do not have the maturity necessary to fully understand the terms of service and privacy policies that must be accepted in order to use the services. The complainants state that as recently as 2018, students were able to freely download apps using their G Suite accounts without restriction on the apps that were available. The complainants state that at that time, when students downloaded apps via the Google App store, there would be an alert that information may be shared with a third party and the students would be the ones to decide whether they allow or deny this.

[134] The complainants also object to the board disclosing information to vendors when new tools are set up. They state that this happens automatically via the accounts connecting with G Suite, regardless of whether the board or the students initiate the accounts.

The board's position

[135] The board again relies on its authority as described in paragraphs 24 through 28

of this report.

[136] The board states that it has the authority to disclose personal information without consent when it is doing so for the purpose for which the personal information was compiled or for a consistent purpose and its disclosure is to an employee or agent and necessary and proper in the discharge of the Board's functions. The board states that its disclosures are permitted under sections 32(c) and 32(d) of the *Act*.

[137] In terms of specific apps, the board states that it does not centrally create student accounts for Duolingo, WeVideo, Infogram, or Powtoon, and consequently, no personal information is disclosed in connection with the use of these tools.

[138] The board advises that students' personal information collected at the time of registration is transferred to Razkids to create accounts for students. The board also discloses personal information to KEV Group for School Cash Online and TVOntario for homework help. The board submits that these disclosures are authorized pursuant to section 32(c) of the *Act*. The board cited sections of the *Education Act* addressing school fees and activities[14], and courses of studies[15], as authority for the disclosures to these third party vendors.

Analysis

Personal information disclosed when setting up student accounts

[139] When accounts are set up, the board discloses personal information to third party vendors.

[140] Section 32(d) of the *Act* permits disclosure to an agent of an institution if the agent needs the information in the course of their duties, and if the disclosure is "necessary and proper in the discharge of the institution's functions." In this case, the third-party vendors are agents of the board, and require the information disclosed to provide their services to and on behalf of the board. The board's disclosures of the personal information in order to set up accounts are necessary and proper in the discharge of its functions. I am satisfied that the disclosure of this information is in accordance with section 32(d) of the *Act*.

Public posts resulting from the use of third party vendor tools

[141] The complainants raise concerns about disclosures that could happen as a result of accepting the terms of use of some of the tools. They provided the example of the Infogram terms of service, which state that a student's username, and all of the content created by the student, would be available for the public to access and view online.

---

[14] *Education Act*, ss. 171(1)23.1, ss.171(1)27, ss.171(1)28 and ss. 171(1)36.
[15] *Education Act*, ss. 171(1)8.1 and ss. 171(1)9.

[142] The board's guidance documents speak to both the issues of disclosures for the vendors' own purposes, and the risks posed by vendors' standard terms of service. Standard terms of service, referred to as "click wrap agreements", are addressed in the "What a Yellow Tool Looks Like" section of the board's Criteria and Considerations for Privacy Reviews, as follows:

> Any application that is solely governed by a 'click wrap' agreement in which the user has no ability to negotiate terms or add privacy protective controls and where some aspect of those terms and conditions are found to be deficient from the privacy viewpoint.
>
> These agreements are not necessarily in the best interests of the board and may include features from the red list above, so some judgement is required.

[143] The board's Criteria and Considerations for Privacy Reviews also states that red tools include those that disclose users' personal information "for commercial purposes or non-educational reasons either by making it public or via third party partnerships."

[144] Public access to content is one of the privacy considerations that the board considered in its assessments of individual tools. Of the assessments provided to me, the only "green" tool that provided public access to content was myBlueprint. That tool allows users to share portfolios only if they actively choose to send the recipient a link to the portfolio. The student also has the ability to password protect the document if they wish.[16] This addresses any concern about personal information being posted without the student's knowledge and without the ability to control who sees it.

[145] One of the complainants' specific concerns was that their child's personal information was posted publicly by Infogram. As this complaint was made anonymously, the board was not able to address the specific public posting the complainants raised, and I am not able to make a finding on whether there was a disclosure contrary to the *Act*. However, the submissions made by the board state that, at least as of June 7, 2019, Infogram is a "yellow" tool, restricted to staff use only, and that student personal information is not to be included on slides that may be created. The board also stated that Infogram does not give public access to content.

[146] I am satisfied that classifying Infogram as a tool for teacher use only, and prohibiting the inclusion of students' personal information in the slides, addresses the general concern of Infogram making student personal information publicly available.

[147] In addition to the use involving YouTube that was addressed earlier, the complainants also stated that YouTube made their child's information public, as it included their personal information with a comment they made on YouTube. The complainants

---

[16] https://help.myblueprint.ca/article/42-how-can-students-share-their-portfolio-s.

stated that their child was under 13 years old at that time, despite YouTube's terms of service state that you must be at least 13 years old to use the service. The complainants refer to the posting of YouTube comments that include students' personal information as a "big privacy breach" and one that the board should have notified other parents about.

[148] Once again, my investigation cannot ascertain this specific allegation because of the board's inability to respond to an anonymous claim. However, more generally, the board has stated that YouTube is now restricted to students 13 years old and above. Of the tools raised by the complainants, YouTube is one of the few[17] that does permit public access to content.

[149] The complainants' position is that the board, via Google, disclosed their child's personal information when their child's name and chosen avatar appeared with a comment the child posted on YouTube. Even if such were the case, I am not satisfied that this would necessarily be a disclosure of personal information by the board or Google, given that it was the child who made the post on the YouTube video. While YouTube allows for video content to be posted privately, a comment on a public video is by its very nature, also public. This is noted in the YouTube Help centre, which states:

> All comments on public videos on YouTube are public and anyone can reply to a comment that you post. If you're a Google Apps account user, any comment you post on YouTube is publicly visible to users outside of your domain.[18]

[150] In general, it is the choice of the individual whether they want to post the comment, and the individual YouTube user should be aware that some of their Google profile information will be displayed in order to attribute that comment. Posting of comments and the associated information would appear to be an act of the user posting the comment, not Google.

[151] I am not satisfied that the board, or the third party acting on behalf of the board, actually disclosed the student's personal information, and so cannot make a finding that this posting of the student's personal information was a disclosure that was not authorized under the *Act*.

Issue 6: Does the board have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal

---

[17] The other is myBlueprint, but as noted in paragraph 143, this tool will only do so if the user actively shares their portfolio(s).

[18] https://support.google.com/youtube/answer/6000964#zippy=%2Cpost-comments-on-a-video.

information of its students, in accordance with the requirements of the *Act* and its regulations?

[152] When an institution contracts with a third party to provide information management functions, there must be contractual and oversight measures in place to ensure that the institution remains in compliance with its obligations under the *Act*.[19]

[153] Under the *Act*, the board is responsible for the security, retention and destruction of personal information in its custody or control.

[154] Ontario Regulation 823, made pursuant to the *Act*, establishes rules that relate to security and retention of records (including records of personal information) in the custody of an institution. Section 3(1) of that regulation addresses the security of records, and requires that institutions define, document, and put in place measures that are reasonable to prevent unauthorized access to the records in their custody or control, including records containing personal information.

[155] Each institution is different, and each may devise their own approach to meeting the requirements in the regulation. This was addressed in Privacy Complaint Report PR16-40, in which Investigator Lucy Costa noted the following:

> [72] From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.
>
> [73] Furthermore, simply because a breach occurred does not by itself mean that reasonable measures were not in place. The standard set out in [*FIPPA* section 4(1)] is not perfection but reasonableness. It is therefore possible for records to be accessed in an unauthorized manner and yet the measures in place still be reasonable.

[156] The focus of the current investigation is on determining whether the board's contractual relationship with third party service providers, as well as its own policies and guidelines, are in compliance with the provisions of the *Act* governing the collection, use, and disclosure of personal information. A further question is whether the board has taken reasonable measures to prevent unauthorized access to the personal information of the

---

[19] Ontario Criminal Code Review Board (C.A.); *Privacy Complaint PR16-40; Ontario Lottery and Gaming Corp. (Re), [2019] O.I.P.C. No. 11.*

students in accordance with the *Act* and its regulations. This latter question engages the board's relationship with all the third party vendors providing it with educational tools or apps.

[157] Where an institution subject to the *Act* retains a private sector entity to provide core functions on its behalf, it must take all reasonable and appropriate measures to ensure that the entity deals with the records under the control of the institution in ways that comply with the institution's obligations under the *Act.* The principal means by which the institution may achieve this objective is through provisions of its contract with the private sector entity that ensure the services performed on the institution's behalf comply with the rules and safeguards set out in the *Act.*[20]

[158] In Privacy Complaint Report PR16-40, Investigator Costa enumerated the contractual provisions relevant to an assessment of whether the institution in that matter had discharged its obligations to ensure that all reasonable steps were taken to protect the privacy and security of personal information under its control. These included provisions relating to:

- Ownership of data
- Collection, Use, and Disclosure
- Confidential Information
- Notice of Compelled Disclosure
- Subcontracting
- Security
- Retention and Destruction
- Audits

[159] The board's main method of ensuring protection of the students' personal information from unauthorized collection, use, and disclosure is through the implementation of its catalogue system. This system includes some measures recommended by the complainants. The board has put restrictions in place as to what apps may be downloaded via the board's app store. Tools that access student information must now be centrally approved by the board, and there are agreements in place for these tools that limit the vendor's collection, use, and disclosure of students' personal information. In addition, the Usage Agreement has provisions that address data deletion, which I will discuss in more detail below. While the complainants' assessment of which

---

[20] Privacy Complaint PR16-40, *Ontario Lottery and Gaming Corp. (Re)*, [2019] O.I.P.C. No. 11 at paras 116-117.

tools have educational value differs from that of the board, one of the board's requirements for the use of a tool is that it support the board's needs. Otherwise, it will be categorized as red and not made available for use.

[160] The complainants observe that many of these changes have occurred since they filed their complaint. I will not be evaluating the adequacy of the previous incarnation of the board's system, but rather, the contractual and oversight measures in the current system.

Contractual Provisions

[161] The catalogue system sets out the following process in evaluating tools:

> Privacy/Security alignment – confirm contact & Non-Disclosure Agreement in place, Privacy & Security Terms & Conditions – in line with HDSB requirements and Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

[162] In earlier submissions, the board stated that as of September 2019, no vendor will be able to connect their tools or apps to the email account of a student of the board unless there is a contract or non-disclosure agreement in place between the vendor and the board. In later correspondence, the board stated as follows:

> The HDSB has curated a catalogue of digital applications (Apps). Beginning in September 2019, the HDSB began restricting the Apps available in the HDSB G-Suite Marketplace for use with students to only those Apps procured and/or reviewed and approved centrally by the HDSB. Apps made available in the HDSB G-Suite Marketplace, which collect personal information, are subject to contractual terms that prohibit ownership of student personal information and restrict disclosure of student personal information.

[163] The board provided me with the contracts it has in place with the vendors that the complainants raised in their submissions. Based on my review of these contracts, it appears that the Usage Agreement is representative of the majority of contractual relationships between the board and third party vendors with access to students' personal information[21]. Given this, my analysis will focus on the obligations within the Usage Agreement, but will also address the previously outlined differences in the KEV Group Agreement's collection, use, and disclosure provisions.[22]

---

[21] The two contracts that differ significantly from the Usage Agreement are the G Suite for Education Agreement and a contract with TVOntario (an agency operated by an Ontario crown corporation). The G Suite for Education Agreement was the focus of a similar analysis in Privacy Complaint MC17-52, and the information practices of TVOntario are not a focus of the complainants' concerns.

[22] See paragraph 102.

Ownership:

[164] The Usage Agreement does not address ownership of the personal information, but does state that any personal information collected, used, retained or disclosed by a vendor in the course of providing services to the board remains under the control and direction of the board. I am satisfied that the board has maintained, as against the vendors, control of its students' personal information and that the vendors do not own this data.

Collection, Use, and Disclosure

[165] The Usage Agreement does not expressly prohibit the use of personal information by vendors for advertising or marketing purposes. Without this prohibition, the board does not have reasonable contractual and oversight measures in place. I have already recommended that the board revise its Usage Agreement (and any similar agreements) to explicitly prohibit vendor use of students' personal information for marketing or advertising purposes, unless the student or parent has identified the personal information in particular and consented to its use.

[166] The Usage Agreement does address collection, use, and disclosure for other purposes, stating that students' personal information may only be collected, used, retained and disclosed by a vendor for the purpose of fulfilling its contractual obligations to the board, and not for any other purpose. The Usage Agreement also states that the vendor may not sell information for its own benefit or purpose.

[167] Of the agreements that I have reviewed, only the KEV Group Agreement does not include these same assurances against use for the vendor's benefit.

[168] The restriction that vendors use the personal information available to them only for board purposes is key to the board ensuring the privacy and security of this information. Without certainty that this provision is included in all of the board's contracts with vendors, I am unable to find that the board has reasonable contractual and oversight measures in place, as required under section 3(1) of Regulation 823.

[169] I have recommended that the board review the agreements in place with vendors of third party tools, identify any agreements that do not provide protections equal to or greater than those found in clauses 5 and 6 of the Usage Agreement, and revise these agreements to provide protections comparable to those clauses.

[170] Implementation of this recommendation, and the recommendation prohibiting the use of personal information for advertising or marketing purposes would bring the board's contractual and oversight measures in line with the requirements under section 3(1) of Regulation 823.

Confidentiality

[171] The Usage Agreement states that a vendor agrees that personal information is defined in accordance with the *Act*, and that any employees and agents of a vendor agree to maintain the privacy of the personal information.

Notice of Compelled Disclosure

[172] There may be situations in which the Vendor may be required by law to disclose personal information to government agencies or similar bodies. In those cases, the Vendor should be obliged to notify the board of this disclosure of personal information. I recommend that the board revise its Usage Agreement to include a clause requiring that Vendors provide notice to the Board of any disclosures of personal information made in compliance with applicable law.

Subcontracting

[173] The Usage Agreement requires that, in addition to vendor employees, agents of a vendor also maintain the privacy of personal information, and execute an agreement confirming the same.

Security

[174] The Usage Agreement states that the Vendor must provide, at the request of the board, confirmation of security features implemented to protect the personal information used and retained by the Vendor "including physical (locked work areas), administrative (training and supervision) and digital (access logs, encryption, password protection)." The Usage Agreement also states that the Vendor's employees and agent who use the personal information must be provided with training. This training is not limited to the security measures, but also includes the parameters for when the personal information may be collected, used, or disclosed. The board may also request confirmation of this training having been provided.

[175] If the Vendor discovers that it has disclosed personal information, the Usage Agreement requires that the Vendor notify the board, and cooperate with the board's privacy breach protocol, intended to contain or remedy the breach.

[176] The complainants raised concerns about successorship, in that vendors may be bought or sold by parent companies. The Usage Agreement does not specifically address this but does state that the terms of the agreement remain in effect with respect to any personal information disclosed to the Vendor, until the personal information is either returned to the board or destroyed. There is nothing in the Usage Agreement to indicate that the obligations on the Vendor cease if the Vendor's business structure changes or the business is sold or changes names. Nevertheless, it would be useful to have certainty on this point. I recommend that the board revise its Usage Agreement by adding a term that ensures the Vendor's obligations regarding personal information will continue to

apply if the Vendor's business name, structure or ownership changes.

Retention and Destruction

[177] The Usage Agreement addresses retention and destruction, stating that:

> The Vendor agrees that upon the conclusion of the business relationship all Personal Information disclosed to the Vendor shall be returned to the Board or destroyed, as determined by the Board. Confirmation of the secure destruction, where Personal Information has not been returned to the Board, shall be provided by the Vendor to the Board in writing within 15 business days following such destruction.

[178] The complainants have stated that they have experienced problems accessing their children's personal information and that student accounts are not closed or deleted at the end of a term or school year. They also stated that the board does not track what personal information vendors have in their possession.

[179] Regarding deletion of data, the board states:

> The Board does not routinely seek verification that personal information collected by vendors is deleted, but may, when its Personal Information Agreement or similar contractual terms exists, seek confirmation from the vendor that personal information has been deleted/destroyed.

[180] The board's Privacy and Information Management Policy includes a commitment to limit the retention of personal information. Section 5 of that policy states that "the use, retention, and disclosure of personal information are limited to the specified purposes identified to the individual, except where otherwise permitted by law."

[181] The provisions of the Usage Agreement provide adequate protection for personal information when the board and the Vendor cease their business relationship. However, none of the provisions raised by the board address what occurs when an individual student ceases using the service, such as when a student graduates or ceases attendance at board schools. This information may well be deleted by vendors based on their individual policies but the Usage Agreement does not contain assurances that this will occur.

[182] The contractual terms in place permit the retention of personal information longer than necessary for the board's educational purposes. In order to remedy this, I recommend that the board revise its Usage Agreement to include both a requirement that vendors delete data for accounts no longer in use and a commitment by vendors to confirm that this deletion had occurred at the board's request.

Audits

[183] The necessity of institutions being able to request audits of the personal

information that they have oversight over was addressed by this office in Privacy Complaint Report PR16-40:

> Audits are another necessary and important way to ensure adequate oversight and compliance with the institution's obligations. Implementation of audits should also be expressly provided for and made enforceable under the terms of the agreement between the institution and the private sector entity.

[184] The Usage Agreement does not include any requirement for vendors to conduct audits.

[185] The board has imposed obligations on vendors through the terms of the Usage Agreement, as discussed above. However, without audit requirements in place, the board is unable to ensure that vendors are abiding by their privacy and security commitments.

[186] I recommend that the board revise its Usage Agreement to include a requirement that vendors perform audits for privacy and security compliance, at the board's request.

[187] Overall, I find that the board does not have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students. I have made recommendations for revisions to the Usage Agreement and to the collection, use, and disclosure provisions of comparable agreements that would strengthen those measures.

CONCLUSION:

1. The student's full name, student number, Ontario Education Number (OEN), grade level, location, email, password, classes, parent's/guardian's email address, performance data, date of birth, enrolment dates, individualized education plan indicator, and photos, as well as work product and similar information about the student obtained in providing educational services, are "personal information" as defined in section 2(1) of the *Act*.

2. The board's notice of collection does not comply with section 29(2) of the *Act*.

3. The use of the personal information used to send marketing or advertising materials to students was not in compliance with section 31 of the *Act*.

4. The board's disclosure of the information at issue was in compliance with section 32(c) of the *Act*.

5. The board does not have sufficient reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students.

RECOMMENDATIONS:

1. The board should revise the current notice in the Statement to include the title, business address, and business telephone number of an officer or employee of the board who can answer questions regarding the collection of personal information.

2. The board should review the agreements it has in place with vendors of third party apps, identify any agreements that do not provide protections equal to or greater than those found in clauses 5 and 6 of the Usage Agreement, and revise these agreements to provide comparable protections to those clauses.

3. The board should revise its Usage Agreement, and any similar vendor agreements, to explicitly prohibit vendor use of students' personal information for marketing or advertising purposes.

4. The board should review which apps in its catalogue use personal information for marketing or advertising purposes, and take the steps needed to prevent the vendors from using students' personal information for those purposes going forward.

5. The board should revise its Usage Agreement to include a clause requiring that vendors provide notice to the Board of any disclosures of personal information it has made in compliance with applicable law.

6. The board should revise its Usage Agreement by adding a term that ensures the Vendor's obligations regarding personal information will continue to apply if the Vendor's business name, structure or ownership changes.

7. The board should revise its Usage Agreement to include both a requirement that vendors delete data for accounts no longer in use and a commitment by vendors to confirm that this deletion had occurred at should the board's request.

8. The board should revise its Usage Agreement to include a requirement that vendors perform audits for privacy and security compliance, at the board's request.

Original Signed by: February 7, 2022

Jennifer Olijnyk
Investigator