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 MC17-52

Toronto District School Board

July 23, 2021

Summary: The Office of the Information and Privacy Commissioner of Ontario (the IPC) received a privacy complaint from the parent of a student of the Toronto District School Board (the board), objecting to the board's use of Google's G Suite for Education services. The complainant alleged that the board's utilization of G Suite for Education contravened the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA* or the *Act*). The complainant's concerns included a failure to notify, and obtain the consent of, parents and children for the collection, use, and disclosure of students' personal information; the use of personal information beyond the scope of what is permitted under the *Act*; the storage of personal information outside of Canada; inadequate security protections for the students' personal information; and a lack of adequate deletion and retention practices for the personal information.

This report concludes that the board's collection, uses, and disclosures of the students' personal information were in compliance with the *Act*, but that the board's notice of collection was deficient.

This report also concludes that the board has reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students. This report makes recommendations to strengthen the board's oversight of those security measures.

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 Report PC08-39; IPC Investigation I94-070M; Privacy Complaint Report MC07-64; Privacy Investigation Report PC12-39; Privacy Complaint Report PR16-40; Privacy Complaint Report MC18-48.

Cases Considered: *Cash Converters Canada Inc. v. Oshawa (City)*, 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 information by the Toronto District School Board (the board). [1]

[2] The complainant is the parent of a child at a school in the board. The complainant alleged that the board allows Google Inc. (Google) to collect, use, and disclose students' personal information in exchange for Google services, in particular G Suite for Education Services, in contravention of the *Act*.

[3] Specifically, the complainant raised concerns that the board had not obtained proper consent for the collection and disclosure of students' personal information to Google and other third parties, has allowed Google to use the information collected beyond the scope of providing necessary educational services, and has not provided proper notice to students and parents/guardians that their personal information is being disclosed to Google.

[4] The complainant also said that he believes that it is a breach of the *Act* to store student information outside of Canada.

[5] The complainant also raised concerns regarding the retention of students' information by Google and the security of the information held by Google.

[6] While the complaint addresses Google's information management practices, the subject of this *MFIPPA* investigation is the school board, and its ongoing accountability, even when it contracts out its responsibilities to a third party service provider. In that regard, the examination of Google is limited to its role as an agent of the school board. A fuller examination of Google's information management practices as a commercial organization subject to the *Personal Information Protection and Electronic Documents Act* is outside this office's jurisdiction.

BACKGROUND:

[7] By way of background, the board has an agreement with Google to provide online educational services that are used by its students and teachers. This service is called G Suite for Education Services[2] (G Suite). The board entered into a Google Apps for

---

[1] References to the "board" in this report will include all of its agents and staff, including teachers.

[2] In January 2018, Google introduced a new version of its services for educational institutions, G Suite Enterprise for Education, available on a fee for service basis, which includes additional data security protections. The Agreement and Addendum pre-date G Suite Enterprise for Education. As the board has

Education Agreement (the Agreement) in August 2011. The Ministry of Education and Google later executed Addendum No. 1 to Google Apps for Education Agreement (the Addendum). The Addendum stipulates that it is incorporated by reference to the Agreement. The board states that the Addendum came into force on August 26, 2013, the day the Ministry of Education executed the document. [3]

[8] When registering with the board, the student is issued a login identification and passcode that can be used to log on to G Suite. The board advised that G Suite services are accessible through a login through the board's portal, and that the board, not Google, authenticates the student.

[9] When students log in to G Suite, the students have access to G Suite services that are provided to the board through its agreement with Google. These services include email, Student Messaging Service, Doc/Sheets/Slides, Sites, Calendar, Drive, Forms, Classroom, and Contacts. These are referred to as the Core Services.

[10] There are additional publicly available Google services that may be accessed using a G Suite account. Google states that these additional services (such as YouTube, Maps, and Blogger) are "designed for consumer users and can optionally be used with G Suite for Education accounts if allowed for educational purposes by a school's domain administrator." [4]

[11] The default setting for the additional services is that they are disabled. The board determines whether students have access to these additional services.

[12] This report will only address students' use of the Core Services and the board's obligations to ensure that the collection, use and disclosure of their information through the Core Services complies with the *Act*. This office is currently dealing with a related complaint that includes the use of the additional services; this report will not address those additional services.

[13] The agreement between the board and Google gives the board administrative controls and discretion, including: creating and deleting user accounts; populating accounts with personal information; creating directories and controlling access; enabling advertisements for subsets of users; adding (or accepting) new features or services beyond the Core G Suite services; and allowing the use of personal devices to interact with the board's portal.

[14] As part of my investigation, I requested and received written representations from

---

not confirmed to me that it is using G Suite Enterprise for Education, I am assuming that the Enterprise version is not in use by the board.

[3] The board signed a copy of the Addendum in 2017, after receiving a request that they provide proof of acceptance of the Addendum.

[4] G Suite for Education Core and Additional services, found at https://support.google.com/a/answer/6356441?hl=en.

the board and the complainant with respect to the complaint, including a copy of the agreement between the board and Google.

ISSUES:

[15] In my investigation I considered the following issues:

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

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 regarding the retention and destruction of personal information of its students, in accordance with the requirements of the *Act* and its regulations?

7. 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*?

[16] The privacy protections under the *Act* apply only to "personal information." Section 2(1) of the *Act* defines "personal information" as follows:

> 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;

[17] 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.[5]

[18] 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.[6]

[19] Personal information is broadly defined in the *Act* to include "recorded information about an identifiable individual". It is reasonable to expect that student evaluation, schoolwork, and emails would contain students' personal information.

[20] The board stated that it uses the student's name to establish a TDSB technology account. The board shares the first and last name of the student when it creates the student's G Suite account and associated email address. While the board states that it does not share the student's school name when creating this account, it agreed that the

---

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

school name is personal information when combined with other information, as it reveals that the individual is a student at a particular school.

[21] The complainant has stated that the information a student adds to their Google account profile is also at issue. The G Suite for Education Privacy Notice (the Privacy Notice) refers to information that may be added to an account profile as "telephone number, profile photo or other information." The board has not provided further details as to what "other information" may be included in the G Suite for Education profile page.

[22] In my view, the name, school name, coursework, emails, and email address meet the definition of personal information as set out in section 2(1) of the *Act*. The board does not dispute this finding.

[23] In addition, I find that a student's telephone number and profile photo meet the definition of personal information as set out in section 2(1) of the *Act*. For the purposes of my analysis, I will assume, without deciding, that "other information" which a student may add to their account profile is also personal information, as defined under the *Act*.

[24] The complainant has stated that more transitory information, such as tracking information and location data, is also at issue. The board and the complainant do not agree as to what, if any, of this additional information is collected, used or disclosed by the board, or Google.

[25] In the Privacy Notice, Google specifies the information that it collects based on the use of its services. This includes:

- device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number of the user;
- log information, including details of how a user used our service, device event information, and the user's Internet protocol (IP) address;
- location information, as determined by various technologies including IP address, GPS, and other sensors;
- unique application numbers, such as application version number; and
- cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

[26] As noted above, Google has access to the names and other personal information of students who use G Suite for Education. When combined with this personal information, the information set out in the Privacy Notice becomes recorded information about an identifiable individual. I am satisfied that the additional information, as set out in the Privacy Notice, is personal information as defined under the *Act*.

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

[27] Section 28(2) of the *Act* sets out the circumstances under which personal information may be collected by an institution:

> Collection of Personal Information
>
> > No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[28] As stated above, in order for a collection of personal information to be permissible, it must satisfy one of the following conditions: it must 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.

[29] 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.

[30] 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* (*Cash Converters*) as follows:

> …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.

[31] 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.

[32] The complainant seems to take the position that any student information that comes into the possession of either the board or Google is a collection of personal information by the board, within the meaning of the *Act*. The board does not agree that its collection of personal information is as broad as that described by the complainant. The question at hand is therefore not limited to whether collection was necessary to the proper administration of a lawfully authorized activity, but also includes a consideration of whether different types of information were collected by the board at all, within the

meaning of "collection" under the *Act*.

[33] The board stated that it collects the student's name at time of registration, and that it does so via the board registration form. The board stated that this collection was compliant with the *Act* and the complainant has not objected to the board collecting student information via the registration form. As such, I will not be addressing the collection of the remainder of the information that the board collects via its registration form.

[34] The complainant's concerns relate to the information Google collects, either on behalf of the board, or for its own purposes, and with any information that the board either discloses to Google, or enables Google to use on behalf of the board or for its own purposes.

[35] Google collects information from students and teachers on behalf of the board. The board advised that it views Google as both a service provider and an agent of the board. The board explained that Google is providing services to the board and is also acting as an agent, as it is authorized by the board to use student personal information for the limited purposes of providing the services under the G Suite agreement.

[36] The board advised that it has not authorized Google to use data or metadata for purposes not related to the provision of educational services.

[37] The board advised that Google, to provide these services, collects certain information from students such as homework, essays, assignments, questions from students to teachers, and communications with students and/or teachers. The board submits that the collection of this type of personal information is to facilitate education activities and falls within its mandate under the *Education Act*. The board advised the collection is necessary to administer its powers and duties pursuant to the *Education Act*, including ensuring that students and staff are following the board's code of conduct for online activity. The board advised that the collection of the students' information is necessary to the proper administration of a lawfully authorized activity pursuant to section 28(2) of the *Act*.

[38] The board states that sections 169.1 to 173, 264 to 265 and 286 to 287 of the *Education Act* set out the various powers and duties of the board, staff, principals and supervisor officers, duties which include the education of students. The board submits that assigning and evaluating work produced by students is a fundamental tool in any educational program.

[39] The board also advised that the board does not collect all of the student information provided within G Suite, and stated that whether the information is collected by the board or not is driven by the context of the interaction. The example provided by the board states that a teacher may "collect" student assignments through G Suite services by requesting that it be submitted through the service. However, the board does not consider a personal email exchange between two students to be a "collection" under

the *Act*.

Contractual Relationship between Google and the board

[40] As I will be dealing with information held by Google, it is necessary to address, as a preliminary matter, the relationship between Google and the board.

[41] The complainant states that the contract between the board and Google is not enforceable, and provides reasons why he believes that the necessary elements of a contract are not present. He also states that both parties have failed to enforce some provisions of the contractual arrangement between them.

[42] He states that this privacy complaint investigation should be paused pending a determination by the appropriate body on the legality and enforceability of the Agreement and Addendum.

[43] Whether this contract is valid or enforceable is a matter between the parties to that contract. The documents on their face establish a contractual relationship. The board has stated that they are both in force. The complainant has not provided any evidence of proceedings between the board and Google in which the validity of the contractual arrangement between the board and Google is at issue. For the purposes of my *MFIPPA* analysis. I am satisfied that these documents form the contractual relationship between these parties, and will treat them as such.

[44] The board described Google as both a service provider and as an agent "authorized by the Board to use student personal information for limited purposes of providing the services under the G Suite agreement."

[45] The complainant has stated that section 13.7 of the Agreement precludes Google from acting as an agent of the board, as it reads as follows:

> No Agency. The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture.

[46] In agreeing to this clause, the parties may well have had their own business objectives. However, nothing in the above term indicates that the parties intended it to have an impact on the meaning of "agency" as it relates to the *Act*, or that they intended to contract out of the *Act*, even if it were legally possible to do so.

[47] I find no contradiction between the above provision and the board's statement that, for the purposes of the service outlined in the Agreement, Google was acting on the board's behalf. As such, I am satisfied that Google is acting as an agent of the board, for the purposes of the *Act*.

Breadth of Student Information within G Suite

[48] Students interact with G Suite in a variety of ways, providing information during

these interactions. A student may work on assignments or other homework, some portion of which is completed and submitted to their teacher. Students may also add information to their G Suite profile. They may send and receive emails, both to other board email addresses or to outside email addresses.

[49] The G Suite Privacy Notice describes the types of information that may be gathered through a student's use of G Suite for Education, which includes the information described above as well as metadata related to the use of Google's services. The "Information we Collect" section states:

> A G Suite for Education account is a Google Account created and managed by a school for use by students and educators. When creating this account, the school may provide Google with certain personal information about its students and educators, which includes a user's name, email address, and password in most cases, but could also include secondary email, phone, and address if the school chooses to provide that information.
>
> Google may also collect personal information directly from users of G Suite for Education accounts, such as telephone number, profile photo or other information they add to a G Suite for Education account.

[50] The Privacy Notice goes on to state that Google collects information based on the use of its services. This information is set out in paragraph 25 of this report, and includes device information, log information, location information, unique application numbers and cookies or similar technologies.

[51] From the above, it is clear that, in providing its Core Services, Google obtains information about students by a variety of different means. It is also clear that some of this information, such as homework which a student places in their G Suite account but does not submit to the board, or metadata about a student's use of the services, may reside in Google's servers, but is never transferred to the board. To the extent that Google gathers such information in the course of providing the Core Services to the board, I will consider whether it is a collection of information by the board and if so, whether it is authorized under the *Act*. I have separated the information gathered by the board and/or Google into different categories, and will address the collection of each type of information individually.

These types of information are as follows:

- G Suite login information
- Emails sent and received by students
- Information from submitted assignments
- Information found in work not submitted

- Tracking, device and other similar information
- G Suite profile information

G Suite login information

[52] I will begin with the type of information the board states it needs to set up a G Suite account: the name and email address of the students. The board has either previously collected this information (the student's name, collected via their registration form) or itself determined the information (student email address). I find that the board does not collect any personal information for the purposes of setting up the G Suite accounts.

[53] The board also states that credentials used for the login process are verified via the board's own server, rather than by Google. I find that any collection of personal information in these credentials by the board is necessary to satisfy the board's responsibility to provide educational services to its students.

Emails sent and received by students

[54] I next turn to the question of whether the information in emails sent and received by the board's students using their G Suite email addresses are authorized collections pursuant to the *Act*. The board has stated that it does not consider at least one subset of this category – namely, a personal email exchange between two students – to be a "collection" under the *Act*.

[55] As such, the first question that must be answered is whether emails sent or received by students are collected by the board. The answer to this is not self-evident, and may vary, depending on the sender, the recipient, and the purpose of the email.

[56] G Suite is not always a direct conduit between the board and the student. It may be in some cases, such as when a student is submitting an assignment, but students may input information into their G Suite accounts that is neither passed on to the board nor utilized by Google. An email sent between students is an example of such information. While this information exists within G Suite, the question is whether this is information collected by the board, either through Google or on its own behalf.

[57] Collection is not defined under the *Act*, but has been previously addressed by this office in the context of emails. In Privacy Complaint Report PC08-39, Investigator Mark Ratner addressed the matter of emails that had been sent unsolicited to those with email accounts at an institution under the *Act*. He noted that the use and disclosure sections of the *Act* refer to personal information having been "obtained or compiled" by an institution and that collection had a narrower meaning, stating as follows:

> I note that personal information may come into the custody or control of an institution in a variety of circumstances: it may be actively solicited, it

> may be passively received, or it may be created by the institution. In my view, the term "obtained or compiled" is intentionally broad, and is intended to accommodate the various ways in which an institution may acquire personal information. This analysis supports the notion that the term "collect" is intended to be interpreted narrowly so as not to apply to situations such as this where correspondence is sent to institutions voluntarily and without solicitation.

[58] In that case, Investigator Ratner determined that the term "collect" did not apply to an institution being sent emails unsolicited.

[59] In the case at hand, emails between the board and its students would be part of an ongoing communication between the student and the board, in the realm of "active solicitation" as described by Investigator Ratner. The board does not dispute that it collects emails sent between students and the board.

[60] However, email correspondence between students, or between students and outside parties, could not be described as being actively solicited by the board, or by Google on the board's behalf. If a message is sent from a student's G Suite account to another student or outside party, without being shared with board staff, there is no evidence that the board has collected that email, as collection is defined under the *Act.*[7] The email may exist on Google servers, having been sent from or received by a G Suite account, but it was not collected by Google on behalf of the board.

[61] This is consistent with access decisions involving personal emails sent by employees of institutions subject to this *Act*. In *City of Ottawa v. Ontario*[8], Justice Molloy stated as follows:

> [G]enerally speaking, I would expect very few employee emails that are personal in nature and unrelated to government affairs to be subject to the legislation merely because they were sent or received on the email server of an institution subject to the Act.

[62] As such, I find that emails sent and received by students via their G Suite accounts and which are not in the normal course shared with board staff, are not "collected" pursuant to the *Act*, merely because they were sent or received on the board's server or the server of its agent. My finding that the board does not collect this type of email eliminates the need to consider whether such a collection would have been "necessary to the proper administration of a lawfully authorized activity", within the meaning of section 28(2) of the *Act*. However, in making this finding, I do not suggest that the board has no responsibility for this information, and in particular, no role in protecting this

---

[7] I acknowledge that there may be exceptional circumstances in which the board collects specific emails between students after the fact, such as when investigating allegations of bullying, but these exceptions may not be in the general course of providing G Suite services.
[8] 2010 ONSC 6835

information from unauthorized access. Below, I address the board's responsibility for the security of this information.

[63] Collection of emails by the board is therefore limited to those emails between students and agents of the board, such as teachers or similar staff. The board described emails of this nature, and its associated email directory, as follows:

> The purpose of the email directory is to permit staff and students throughout the board to communicate with one another on a wide range of activities including class assignments, homework, intermural sports and other extracurricular activities.

[64] The board noted that communications between students and teachers were authorized pursuant to the *Act*, stating as follows:

> …the school notes that G Suite accounts are used to facilitate a wide variety of educational activities including communications between students themselves and with teachers on issues related to class projects, deadlines, homework assignments, and other such related activities. The board notes that its general powers and goals are described in section s. 169.1 through s. 173 of the *Education Act* and encompass its mandate to provide education to pupils in Ontario.

[65] I am satisfied that the collection of emails between students and board representatives, including teachers and other staff members, is necessary to satisfy the board's responsibility to provide educational and associated services to students.

Information from submitted assignments

[66] This category of information includes assignments, projects and other schoolwork submitted by the student via G Suite, and collected by Google on behalf of the board.

[67] These assignments are work requested by teachers or other agents of the board, as part of a student's coursework. They are in turn provided to the board, via G Suite. Assignments and similar coursework submitted by students to the board are clearly a collection by the board under the *Act*.

[68] The remaining question is whether that collection by or on behalf of the board is necessary to the proper administration of a lawfully authorized activity.

[69] With respect to the question of whether the collection of personal information by or on behalf of the board is necessary to the proper administration of a lawfully authorized activity, the board has referred to its powers and obligations under the *Education Act*, including providing an education to board students. The board explained that assigning and evaluating work produced by students is a fundamental tool in any educational program and that G Suite was implemented to assist in providing educational services.

[70] The board's explanation is consistent with the analysis in IPC Investigation I94-070M, in which then-Commissioner Ann Cavoukian confirmed that the assignment of projects, and the associated collection of personal information, was necessary for the administration of a school board's lawfully authorized activities.

[71] I am satisfied that assigning and evaluating work production as well as providing instruction are lawfully authorized board activities. I am also satisfied that the collection of this work product is necessary to the administration of these lawfully authorized activities.

Information found in work not submitted

[72] Unlike the above category, this information does not include students' work product that students directly communicate to the board. Instead, it includes only that work product that the student has chosen not to share with the board.

[73] One of the G Suite features available to students is file storage, provided via Google Drive. This allows students to submit schoolwork by uploading it, but also allows for storage of other documents such as working drafts of papers that the student has not submitted. The board, in its representations, noted that documents in Google Drive may be kept private, or shared with those within or outside the board, at the student's preference. As such, a student's Google Drive folder may contain schoolwork or other documents that have not been submitted by the student to the board.

[74] In my view, as with student emails not sent to or from the board, this non-submitted work has not been "collected" by the board. These types of documents may be present on Google's servers, but there is no indication that the board actively solicits their creation. There is likewise no indication from the board that they retrieve such documents from G Suite, without the student themselves submitting them.

[75] Rather, these are documents that students generate and store, using the tools available to them. Such documents appear to be wholly within the control of the student, and not the board. As such, I am satisfied that documents not submitted to the board, but stored on Google's servers, are not a collection of personal information by the board pursuant to the *Act*. Again, my finding that the board did not "collect" this information does not lead to a conclusion that the board has no responsibility for it, as discussed below.

Tracking, device and other similar information

[76] The complainant has expressed concerns about information obtained from students that is associated with the use of a particular device or is similarly transitory in nature. I have previously found that this type of information, when combined with other information that identifies students, is personal information.

[77] The Privacy Notice, as excerpted at paragraph 25 of this Report, provides a list of

potential data collected. This includes device information, log information, location information, and cookies or similar technologies, the "metadata". While in a conventional sense the board does not strictly speaking "collect" this metadata, it is generated as part of the creation or transmission of content that the board does collect, such as student assignments or emails from students to teachers. I find that Google collects this information on behalf of the board, in providing its services.

[78] It is important to read the Privacy Notice together with the Agreement between the board and Google, since the Agreement is the primary document setting out Google's obligations in providing its services to the board, and prevails over the Privacy Notice. As discussed further below, that Agreement restricts Google's use of any student information, including this kind of metadata, to specified purposes, all related to the provision of the services. With those restrictions, I accept that in order for Google to provide the G Suite services, a certain amount of activity tracking and monitoring is necessary. As such, I find that the collection of the type of information listed in the G Suite Privacy Notice is necessary for the administration of the board's lawfully authorized activities.

G Suite profile information

[79] Google provides a profile with each G Suite account. This profile includes categories of information associated with that student account that are generally accessible to other users of the system, such as their name, grade, and email address. The student has the option of filling in the information in this profile, as noted in the Google Privacy Notice as follows:

> Google may also collect personal information directly from users of G Suite for Education accounts, such as telephone number, profile photo or other information they add to a G Suite for Education account.

[80] The questions at hand are whether providing a profile, and obtaining information via that profile, is a collection pursuant to the *Act*, and if so, whether this collection is necessary to the administration of a lawfully authorized activity of the board.

[81] Much like the emails sent to parties other than the board, and the work not submitted to the board, there is a question as to whether this information is collected pursuant to the *Act*.

[82] As noted in the board's materials, G Suite is a means by which students can access a range of services including, but not limited to, the Core Services. The complainant has cited this range of services as a reason why students may want to provide as little information as possible. This is certainly true for the complainant, and may well be true for many others. However, this wide range of applications could equally be a reason for a student to take advantage of this profile section to provide additional information about themselves. For example, they may wish to post a picture to give a face to a name, or provide additional contact information. It makes sense to have a place to put this

information, such as the profile section.

[83] The provision of this information is entirely up to the student and/or their parent, and is unsolicited by the board. There is no evidence that the information inputted into this section is provided to the board, or that Google collects it on behalf of the board. It appears that this information is kept in Google's servers, as with emails which do not involve board staff, and unsubmitted work.

[84] I do not consider that, by simply providing a place for this information, the board is collecting that information. Nor is Google collecting that information on behalf of the board. A physical comparison may be to a bulletin board at a school. The school may put the bulletin board up, but it is not collecting any information that students may choose to post on that board.

[85] As such, I am satisfied that the student information in the profile section, which is not submitted to the board but stored on Google's servers, is not a collection of personal information pursuant to the *Act* by Google on behalf of the board. However, consistent with my statements above, the board has a responsibility to protect it against unauthorized access.

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

[86] 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.[9]

[87] 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

[9] PC12-39, page 10.

> (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.

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

[89] The complainant advised that when he initially asked to see the notice of collection, the board was unable to provide one. The complainant stated that the board later advised parents that it did not have a notice in place but that notice would be provided starting in September 2018. The complainant said that he was never provided the notice by board staff.

[90] In the course of my investigation, the complainant viewed the notice provided to the IPC by the board. The complainant does not believe that the notice provided complies with the *Act*. In addition, the complainant raised concerns that the notice provided by the board is difficult to find, as the complainant was unable to find the notice on a mobile web browser. The complainant also advised that students and parents did not receive the notice directly. The complainant believes that the notice is not readily accessible to the general public and fails to meet the requirements of section 29(2).

The Board's Representations:

[91] The Board provided a copy of the notice along with its submissions. The board also advised that the notice can be found on its website, and that it identifies the purpose of G Suite, sets out the legal authority for the collection and the contact information. There is a more current version of the notice on the Digital Learning Tools section of the board's website[10] and as such, I will address the most current version.

[92] The Digital Learning Tools section states that the board provides students with a variety of digital learning tools, which are "carefully selected for their educational value and compatibility with the Ontario Curriculum to support and enhance learning." This page includes a description of G Suite and provides an explanation of the board's use of G Suite, stating:

> TDSB has a contractual agreement with Google for G Suite for Education which is significantly different from a personal Google account anyone can create. The agreement provides TDSB with content ownership, application controls & support and protection from advertisements.

[93] This section also sets out the Core G Suite applications, indicates which grades have access to which application, and states that each student at the board has a G Suite

---

[10] Found at https://www.tdsb.on.ca/High-School/Your-School-Day/Technology/Digital-Learning-Tools, Current to June 14, 2021.

account.

[94] The privacy notice found on the website (the Learning Tools Notice) reads as follows:

> Some digital learning tools require that the TDSB share limited personal information such as the student's name and email address for the purpose of creating an account to use the tool or service. Any content created in and/or stored in a district provided digital learning tool remains the property of TDSB. Personal information (name and email address) is used and shared by the TDSB for the above-noted purposes under the authority of subsection 11(3) and section 20 of the Ontario Regulation 298, R.R.O *Education Act, R.S.O. 1990, c.E.2.* The information is retained in accordance with the *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56*.
>
> If your question is not answered by the resources on this page, please contact your school principal or [name of employee], Senior Manager, Client Relations, IT Services [board email].

Analysis:

[95] 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.

[96] The board, in its representations, took the position that it only directly collected the student's name, and did not collect other information that Google obtained in the course of students using G Suite. I have found above that Google, on behalf of the board, collected other personal information, including emails to and from the board, and school assignments. I have also found that tracking, device, and other similar information collected by Google is personal information as defined under the *Act*.

[97] The Learning Tools Notice is silent on the authority for the collection of personal information. The notice cites authority for the personal information that is being "used and shared" by the board, but does not provide a similar authority for the collection of the personal information. Accordingly, I find that the notice published on the Digital Learning Tools section of the board's website is not in accordance with section 29(2) of the *Act*.

[98] I provided the board with a draft version of this Report, in which I stated that the board could remedy this deficiency by revising the notice of collection to include the authority for the collection of the personal information by the board via G Suite. The board provided a revised Notice of Collection to the IPC, which implements this recommendation.

[99] Regarding the remaining notice requirements, the notice states that the board shares "limited personal information" with its digital learning tools, such as G Suite, and states that this information is used for the purposes of supporting and enhancing learning. It also cites the authority for its use and includes the business contact information for an employee who can answer questions regarding this information. In addition, the notice states that "[any] content created in and/or stored in a district provided digital learning tool remains the property of TDSB." This description includes the broader range of information held by Google due to the students' use of the G Suite services, regardless of whether some of this information may be collected, within the meaning of the *Act.*

[100] I note that the complainant stated that notice was not provided by the board until September 2018, and that the notice provided since that time was insufficient, as it was difficult to find online.

[101] If the board failed to provide notice prior to September 2018, this was a contravention of notice of collection provisions of the *Act*. However, any possible non-compliance has largely been resolved by the posting of the existing notice, and will be resolved in its entirety if the board adds the authority for its collection of personal information to the existing notice.

[102] I cannot speak to whether previous versions of the notice were difficult to find, and as such, effectively inaccessible. I was able to locate the current version, by performing an internet search for the terms "TDSB" "G Suite" and "privacy".

[103] However, I do note that not all parents may be aware of the use of G Suite, and may not visit the Digital Learning Tools section of the board's website. Including the notice within materials provided to each student's household, such as a registration package, would ensure that all parents receive the notice of collection. Accordingly, I recommend that the board revise the current notice as they have indicated, and also include a copy of this revised notice within students' registration packages.

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

[104] 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*.

[105] 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.

Complainant's position:

[106] The complainant argues that students' personal information is not being used for the purpose for which it was obtained or for a consistent purpose, and therefore the board does not have the authority to use the information.

[107] The complainant notes that although the board states that it does not allow Google to use the information for its own purpose, the addendum to the agreement appears to allow Google to "operate" and "enhance" its infrastructure using personal information as defined under section 2(1).

[108] The complainant noted that under the section "Use of Customer Data" of Addendum No. 1 it states the following:

> 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;

[109] In addition, the complainant notes that Google's general privacy policy section titled "Maintain & Improve our services" states:

> And we use your information to make improvements to our services — for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

[110] Based on the above excerpts, the complainant believes that the board has given Google the authority to use the student's personal information beyond the purpose of providing educational services.

[111] The complainant believes that student information should not be permitted to improve another organization's infrastructure, as the *Act* says that the information can only be used for its intended purpose. The complainant argues that allowing Google to use student personal information to enhance and support Google's infrastructure could result in Google using the personal information to build new software or improve the

current software, which may include training Google's artificial intelligence algorithms.

[112] In addition, the complainant believes that the board's agreement to the contract with Google, the terms of service, privacy notices and privacy policies, go beyond the authority granted under the *Education Act*. The complainant argues that the *Education Act* imposes limits on the board with respect to using personal information in the delivery of education services and does not include allowing Google to use the data to enhance and operate its infrastructure.

[113] The complainant also states that Google avoids disclosing the ways that it uses personal information and that the IPC's underlying assumption should be that Google is collecting and using personal information in ways that violate the *Act*.

The Board's Position:

[114] The board's position is that it has the authority under the *Act* to use student information for G Suite Services and has taken steps to ensure that Google uses the information in a manner compliant with the *Act*.

[115] The board entered into a Google Apps for Education Agreement in August 2011. It provided the IPC with a copy of the Agreement.

[116] The board advised that in order to ensure that Google uses student personal information in a manner compliant with the *Act*, the board and Google also executed Addendum No. 1 to Google Apps for Education Agreement. The Addendum was created by the Ministry of Education and stipulates that it is incorporated by reference to the Agreement.

[117] The board advised that the use by the board of the school name and the name of students to set up a student email address is in accordance with section 31(c) in conjunction with section 32(d) of the *Act*.

[118] The board advised that it offers the G Suite service as a tool to students and teachers to facilitate the administration of educational activities within the board, as described earlier. The collection and use of the information is for the purposes of educational activities and is necessary for the administration of a lawfully authorized activity.

[119] The board advised that Google is explicitly prohibited from using the information for its own purposes or other purposes not identified. Google's use of the personal information is restricted to the purposes identified in item 4 of the Addendum. The board said that these purposes are to facilitate the provision of G Suite to the board, its students and teachers.

[120] The board noted that the Privacy Notice states that the personal information collected when users are using the Core Services is used only to provide the Core Services.

It also states that Google does not serve advertisements in the Core Services or use personal information collected in the Core Services for advertising purposes.

Analysis:

[121] As noted in previous investigations by our office, in order for a given use of personal information to be permissible under the *Act*, the institution in question must demonstrate that the use was in accordance with a least one of the section 31 exceptions.

[122] With respect to the student personal information that is used for the G Suite services, the board has taken the position that the use of student information is in accordance with section 31(b), in that it states that the use is for the purpose for which it has been obtained or compiled, or for a consistent purpose.

[123] As explained in Privacy Complaint Report MC07-64, when determining whether a particular use of personal information is in accordance with section 31(b), it is first necessary to determine the original purpose of the collection. Next, it is necessary to assess whether the use of this information can be properly characterized as being either for the original purpose of the collection, or for a purpose that is consistent with that original purpose.

[124] I have already determined that the purpose of the collection of the student information is to assist teachers with assigning and evaluating work production, to provide instruction, and to assist in communications with students. Though the information collected by the board is diverse in its nature, ranging from device information to emails to coursework, it was all collected for these permissible purposes.

[125] While the board cited section 31(c) as the authority for its collection of the student names and school names, this information was also collected to provide educational services to the students. Accordingly, the first criteria of the section 31(b) test is met for the student information collected by the board.

[126] The next step in the section 31(b) analysis is to determine whether the use was for the original purpose of the collection or for a purpose that was consistent with that original purpose.

[127] The board's use of a student's name in the creation of a G Suite account allows students to participate in educational services provided by the board. Accordingly, I also find that the board's use of a student's name to create a G Suite account is for the purpose for which it was obtained or compiled or for a consistent purpose, and is therefore in accordance with section 31(b) of the *Act*.

[128] Before moving forward to address the use of the personal information in the Customer Data, I want to address one point made by the complainant. Part of his contention throughout this matter has been that due to Google's past conduct in various spheres, the IPC should assume that Google is using personal information for purposes

that it has not disclosed and that are not authorized under the *Act*.

[129] As evidence of this, the complainant referred me to matters outside of the sphere of this investigation. Without commenting on the incidents themselves, I will note that they do not involve the personal information at issue within the scope of this report. I cannot base my findings on assumptions unsupported by evidence applicable to the matter before me. The information before me is that the board entered into a relationship with Google under which it would provide G Suite services to the board. These services were to be provided in accordance with contractual protections between those parties, over and above any protections Google may offer via its free services, as those protections are documented in the Privacy Notice. These protections include limitations on the use of Customer Data as set out in the Addendum.

[130] The board entered into this Agreement with Google, including the Addendum, with the expectation that Google would abide by these conditions. I therefore accept that the contractual relationship establishes the boundaries of Google's permitted use of this data, and this will form the basis of my analysis going forward. An examination of Google's personal information management practices writ large is beyond the scope of both this investigation and this office's jurisdiction.

[131] The conditions on the use of Customer Data, as set out in the Addendum, are:

> (a) to provide the Services; (b) to operate, maintain, enhance and support the infrastructure used to provide the Services; and (c) comply with Customer's or End Users' instructions in the use, management and administration of the Services; (d) to respond to customer support requests.

[132] The Customer Data was collected by the board and/or Google so that G Suite services may be used to facilitate the administration of educational activities within the board. All of the uses set out in item 4 of the Addendum are either for the purpose for which the personal information was obtained or compiled or for a consistent purpose.

[133] I note that the complainant has objected in particular to Google using the Customer Data "to operate, maintain, enhance and support the infrastructure used to provide the Services," especially in light of the Privacy Notice, which states that Google may use the information it collects to develop new services. This Privacy Notice also states that Google may combine personal information from one Google service with another.

[134] While the general G Suite Privacy Notice allows for broader uses of personal information than set out in the Agreement, the documents that govern the specific G Suite services provided by Google to the board are the Agreement, and the Addendum which is incorporated into the Agreement. The "Use of Customer Data" section of the Addendum states that "Google will only use Customer Data in accordance with this Agreement."

[135] The term of the Agreement itself limits the operation, maintenance, enhancement,

and support to the infrastructure used to provide the core G Suite services. This prohibits Google from using the Customer Data directly to improve its other services, beyond the Core Services.

[136] The complainant alleges that such use may improve other Google services. Even if it were so, and the use of Customer Data to improve the Core Services necessarily resulted in the improvement or enhancement of other services, such a use would still be consistent with the original purpose of collection. The mere possibility that it may also have an incidental side effect of improving other services does not render the use impermissible under the *Act*.

[137] Accordingly, the complainant's concerns arising from the Privacy Notice are resolved in this case by the Agreement, which constrains the use of the Customer Data to the four categories of uses set out in the Addendum's Use of Customer Data section.

[138] I find that the use of the students' personal information included in the Customer Data, by the board and/or Google, is for the purpose for which it was obtained or compiled or for a consistent purpose, and as such, is in accordance with section 31(b) of the *Act*.

[139] As I have found that the student information is used in accordance with section 31(b) of the *Act*, it is not necessary for me to address whether that use is also in accordance with section 31(c), as claimed by the board.

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

[140] 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.

[141] 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;
> >
> > (d) 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 Complainant's Position:

[142] The complainant's position is that the board has violated the *Act* by disclosing students' personal information to Google, a third party, without authority and in particular, without consent. The complainant contends that section 32(b) of the *Act* requires consent to be obtained when there is a disclosure.

[143] The complainant believes that the IPC's underlying assumption should be that Google is collecting and using personal information in ways that the board has not identified. The complainant states that the board has not obtained students' and parents' consent for the disclosure of this information to Google.

Board's position:

[144] The board advised that it relies on section 32(d) of the *Act* with respect to the information that is shared with the board's IT staff in order to establish the student technology account and shared with Google to establish a G Suite account.

Analysis:

[145] While the complainant objects to disclosure on the basis of lack of consent, section 32(d) contains no consent requirement.

[146] The board states that the disclosure is limited to the information necessary to establish the student technology account and G Suite account. While the complainant contends that the board discloses additional information to Google, I cannot assume that this is the case. When addressing the collection of data, it was clear from the board's description of the G Suite services that Google itself was collecting Customer Data in the provision of these services, beyond the personal information the board shared with it. It is not apparent that there are similar additional disclosures to Google. The board has identified the information that it disclosed to its staff and to Google, and my findings will be limited to that identified data.

[147] Section 32(d) has been considered by the IPC in a number of previous Privacy Complaint Reports. Generally, the IPC decisions identify three criteria for the application of this exception. The criteria are as follows:

1. the disclosure must be made to an officer, employee, consultant or agent (Investigation Report I96-113);

2. who needs the information in the performance of their duties (Privacy Complaint Report MC-050034-1 and Order PO-1998); and

3. the disclosure must be necessary and proper in the performance of the institution's functions which includes the administration of statutory programs and activities necessary to the overall operation of the institution (See, for example, Investigation Report I95-007M).

[148] Section 32(d) makes it clear that a disclosure of personal information even within an institution must be justified and will be subject to scrutiny on a "need to know basis." The sharing of information within an institution must be based on more than "mere interest or concern" [for example, see: *H. (J.) v. Hastings (County)* (1993), 12 M.P.L.R. (2d) 40 (Ont. Ct. Gen. Div.]. There must be a requirement for the personal information to be disclosed in order for individuals to carry out their duties and ensure the performance of the institution's functions.

[149] The board has submitted that Google is its agent and is authorized by the board to use student personal information for the purposes of providing the services under the G Suite agreement. The board has a formal agreement with Google that sets out the services to be provided and the protections that must be in place. It has already been established that part of the board's functions is to provide educational programming to students. The board has submitted that Google requires the personal information in order to perform its obligations and duties pursuant to its contract with the board.

[150] I find that disclosure of the student information used to set up the G Suite accounts was necessary in the discharge of the board's functions.

[151] In this case, Google is an agent of the board and requires the information to provide the Core Services. The disclosure of the information needed to establish the student technology account and G Suite account from the board to Google is necessary and proper in the discharge of the institution's functions. I am satisfied that the disclosure of the information at issue was in accordance with section 32(d) of the *Act*.

Issue 6: Does the board have reasonable contractual and oversight measures in place regarding the retention and destruction of personal information of its students, in accordance with the requirements of the *Act* and its regulations?

[152] Section 5 of Ontario Regulation 823, made pursuant to the *Act* , sets out the retention requirements for records of personal information in the custody or control of an institution and states:

> Personal information that has been used by an institution shall be retained by the institution for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, unless the individual to whom the information relates consents to its earlier disposal.

[153] This provision establishes a minimum one year retention period (or less when set

out in a by-law or other resolution of the institution) for personal information that has been used.

The Complainant's Position:

[154] The complainant takes the position that the agreement between the parties effectively gives Google the final determination as to when student data is destroyed, and allows for Google to not fully dispose of the data.

[155] The complainant acknowledges that the Addendum addresses the destruction of data, but notes that it does not address back up servers, and that the Privacy Notice seems to allow for longer retention of data on such servers, as it states "there may be delays when you delete something and when copies are deleted from our active and backup systems."

[156] The complainant states that the Agreement and the Privacy Notice fail to specify the type of data that is deleted, or the method of deletion. The complainant contends that language in the privacy notice regarding deletion is ambiguous, it refers to "deletion of personal information consistent with the functionality of our service", the meaning of which is unclear. The complainant contends that this wording, and general ambiguity in the contractual terms, allows Google the ultimate discretion as to when and if data is deleted.

[157] The complainant also states that the board itself fails to give prompt instructions to Google to destroy the data, and so allows Google to retain the data for longer than is necessary. The complainant believes that when a student deletes data on G Suite, the actual deletion does not take place until after the student has left the board, which could be years later. The complainant bases this on the board telling parents that it initiates the deletion of a student's account some months after the student has left the board. The complainant believes that this is well beyond any data retention requirements.

[158] I note that the complainant's arguments highlighted discrepancies between the Addendum and Google's Privacy Policy. These arguments are not outlined here because the Privacy Notice states that where terms differ, the Agreement (as amended, via the Addendum) takes precedence, followed by the Privacy Notice and then Google's Privacy Policy.

The Board's Representations:

[159] The board advised that it deletes G Suite accounts upon request or when a student graduates or transfers out of the board. The board noted that under the Addendum, Google is required to delete the student's data from its servers upon the deletion of the account by the board.

[160] Once the board makes a deletion request, the product or service containing the data at issue follows a deletion process.

[161] The board states that students may opt out of G Suite services at any time. The board advised that if a student opts out, their Google account is deleted including any data that was created and/or stored in the account. The student will no longer appear in the board's email directory. The student retains a board technology account enabling them to log on to the board's wired and wireless networks and access other technology resources and digital learning tools provided by the board, such as board-owned computers and the board's virtual library.

[162] Regarding these opt-out provisions, I note that the complainant raised a concern that the board merely allows students to opt out of G Suite services, without providing an alternative service. The complainant stated that this is a violation of its obligation under the *Education Act* to accommodate, and therefore believes that the board is not permitted under that legislation to employ G Suite services.

[163] I have already addressed the board's authority to collect, use, and disclose student data, which does not require student or parental consent under *MFIPPA*. Nor does the *Act* require institutions to offer viable alternatives. The question of whether the board has met its obligations of accommodation under the *Education Act* is a matter outside the scope of this office's authority, and will not be addressed further.

[164] The board advised that it can also delete Customer Data at any time. The board advised that when Google receives a complete deletion instruction from the board (such as when an email the board has deleted can no longer be recovered from the "trash"), Google will delete the relevant Customer Data from all of its systems within a maximum period of 180 days unless retention obligations apply. The board stated that Google's commitment to the 180-day period can be found in its "Google Workspace & Google Cloud Platform Commitments to the GDPR [General Data Protection Regulation]."[11]

[165] The board also advised that replication servers contain copies of data so that, in the event of a disaster affecting one server, the customer's data is still available via the replication servers.

Analysis:

[166] The board has not indicated that it has passed a bylaw or resolution regarding records containing personal information, so I will assume that the one-year minimum retention period, as set out in section 5 of Ontario Regulation 823 applies to these records. I further assume that the board retains the records of personal information for this minimum period, unless the individual to whom the information relates has consented to its earlier disposal, as required by section 5(b) of the regulation.

[167] The board takes the position that Article 5 of the Addendum requires Google to delete the student accounts from its servers upon the deletion of the account by the

[11] https://cloud.google.com/security/gdpr.

board.

[168] Section 10.3 of the Agreement provides that if the Agreement is terminated, after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active and replication servers and overwriting it over time. In addition, upon request, each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.

[169] Section 5 of the Addendum adds the following sentence to the end of section 10.3:

> Upon Customer deleting data, Google will delete the data and pointers to the data from active servers and replication servers.

[170] I note that section 10.3 is entitled "Effects of Termination", which raises the question of whether the commitments in section 5 of the Addendum apply while the Agreement is in force, or only after the Agreement has terminated.

[171] While the title of the section is a factor to consider, it is not determinative of the issue. Section 10.3 is the only part of the Agreement that addresses deletion of Customer Data. The section 5 commitments may have been inserted there simply for that reason.

[172] Section 10.3(iii) of the Agreement already states that "If this agreement terminates, then… after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active and replication servers and overwriting it over time." If the Section 5 commitments applied only after termination of the Agreement, they would be entirely redundant.

[173] Taking all these factors into consideration, I find that the section 5 commitments apply both while the Agreement is in force and after it has terminated.

[174] In addition, Google has stated its commitment to deleting Customer Data within 180 days of a complete deletion request, as set out in "Google Workspace & Google Cloud Platform Commitments to the GDPR."[12] Taken together with the Agreement, this provides sufficient assurance that Google will destroy Customer Data within 180 days of either the termination of the Agreement or a complete deletion instruction.

[175] I appreciate that the complainant believes these commitments to be insufficient. However, the board has confirmed that if a parent or student requests that an account be deleted, that deletion occurs immediately, rather than being delayed until a student leaves the board. The 180-day commitment made by Google is the maximum time deleted data may remain prior to deletion; this deletion may occur much sooner. I accept that

---

[12] The complainant notes that the GDPR was not in place at the time he filed his complaint with the IPC. However, the commitments noted in "Google Workspace & Google Cloud Platform Commitments to the GDPR" are currently applicable, and therefore relevant to the analysis of the board's contractual and oversight measures currently in force.

when a data deletion request is made to Google, that data is destroyed within a commercially reasonable time.

[176] Based on the above, I find that the board does have reasonable contractual and oversight measures in place regarding the retention and destruction of the personal information of its students.

Issue 7: Does the board have reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of students using the G Suite services?

[177] Prior to addressing the board's contractual and oversight measures regarding privacy and security, I want to clarify the extent of the personal information those measures protect.

[178] Earlier in this report, I set out which student personal information was collected by the board or by Google on behalf of the board, and which information was held within G Suite, but not actually collected by the board. That distinction was necessary to determine which personal information the section 28 collection provisions apply to.

[179] Neither Google nor the board makes this distinction regarding their security obligations. The contractual arrangement between Google and the board does not limit Google's privacy and security obligations to the information that was "collected," within the meaning of the *Act*, either by the board or by Google on behalf of the board. As will be discussed in more detail below, Google's obligations apply much more broadly, including to all personal information it harbours on its servers as a result of its contractual relationship with the board.

[180] This contractual arrangement mandates that Google's obligations to protect personal information extend not just to the information collected by Google or the board, but to all personal information that is "provided, generated, transmitted, displayed, or stored" via G Suite. This includes personal information within G Suite not collected by the board, such as a student's profile information, as well as any emails sent to or received from parties outside of the board.

[181] Accordingly, the below analysis of the board's contractual and oversight measures is not limited to only the personal information that the board collects, but extends to all student personal information within G Suite.

[182] 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*.[13]

---

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

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

[184] 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 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.

[185] 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 at paragraphs 72-73:

> [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.

[186] This investigation is not reviewing a specific breach. The current investigation is to determine whether the board has the authority to collect, use and disclose information to the third party, in this case Google, and if so, have they taken reasonable measures to prevent unauthorized access to the personal information of the students in accordance with the *Act* and its regulations.

[187] Where an institution subject to the *Act* retains a private sector entity to perform 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 that the services performed on the institution's behalf

comply with the rules and safeguards set out in the *Act.*[14]

[188] In order to determine whether the measures in place in a given institution are reasonable, it is necessary to consider the contractual arrangement in place. In this case, the board and Google entered into the Agreement, which incorporates the Addendum and the Attachment.

[189] The IPC has developed an approach to determining whether an institution has sufficient contractual and oversight measures in place where it retains a private sector entity to perform functions involving the handling of personal information within its control. This is set out in PR16-40 as follows:

> [117] The above-noted principles and examples of the types of contractual provisions which should be in place for records of personal information are described in Privacy Investigation Report PC12-39, *Reviewing the Licensing Automation System of the Ministry of Natural Resources, A Special Investigation Report* (MNR Report). One of the issues considered in that report was whether an agreement with a private sector company for the operation of the Ministry of Natural Resource's hunting and fishing Licensing Automation System (LAS) was adequate for the purposes of the *Act*. The relevant passages are set out here.
>
> **The Contract**
>
> ... Organizations must take reasonable steps to reduce the likelihood of a breach, wherever the information may be held. This becomes especially important when government information management functions are outsourced to private sector agents. In these cases, the reasonable measures required under the *Act* and its regulations include appropriate contractual provisions that ensure accountability, privacy and security. Therefore, whether the Ministry has discharged its obligations to ensure that all reasonable steps have been taken to protect the personal information under its control must be assessed in view of its agreement with the Agent.
>
> I have carefully reviewed the Ministry's agreement with the Agent, including the contract and all appendices and schedules. The Ministry's contract includes robust provisions that protect the personal information under its control and restrict the use of that information by the Agent.

[190] In PR16-40, Investigator Lucy Costa, following the approach set out in Privacy Investigation Report PC12-39, addressed the contractual provisions relevant to an

---

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

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
- Governing Law

The agreement between the board and Google:

[191] I have carefully reviewed the Agreement, including the Addendum and the Attachment. The board explained that Google and the Ministry of Education collaboratively created and committed to the Addendum. The Agreement was signed by the board and Google in August 2011. The board advised that the Addendum and Attachment came into force on August 26, 2013.

[192] It is important to note that the G Suite for Education Privacy Notice stipulates that the G Suite for Education agreement takes precedence, if the terms of the Privacy Agreement and the Agreement (as amended) differ.

[193] As in the contract discussed in Privacy Investigation Report PC12-39, the Agreement contains a number of provisions relevant to the privacy and security of personal information. I will address each in turn. To the extent that some of these provisions raise other related issues, I will also address those in the following discussion.

Ownership:

[194] Section 6.1 of the Agreement provides that the Customer owns all intellectual property rights in Customer Data. Section 2 of the Addendum states that ”Customer or End Users, as applicable, own all Customer Data”.

[195] Without determining the extent of the board’s rights vis-à-vis its students, it is clear that the board has not yielded control of this information to Google. I conclude that

the board has maintained, as against Google, control of its students' personal information and that Google does not own the Customer Data.

Collection, Use, and Disclosure:

[196] Item 4 of the Addendum provides that Google will only use the Customer Data for four purposes: (a) to provide the Services; (b) to operate, maintain, enhance and support the infrastructure used to provide the Services; and (c) comply with Customer's or End Users' instructions in the use, management and administration of the Services; (d) to respond to customer support requests.

[197] The board has advised that Google is not permitted to collect or use information in its G Suite services for advertising purposes or to create ad profiles.

[198] Section 5.1 of the Agreement provides that each party (including any affiliates, employees and agents to whom it had disclosed Confidential Information) may use the information only to exercise that party's rights and fulfill its obligations under the Agreement, while using reasonable care to protect this information. Each party is responsible for any action of its affiliates, employees and agents in violation of this section. Customer Data is included under the Agreement's definition of Confidential Information.

[199] Section 5.1 also provides that each party will not disclose Confidential Information, except to affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential.

[200] The board was asked whether it was aware of which of Google's affiliates may be accessing the information and for what purpose. The board advised that affiliates may be involved in the processing of Customer Data for the purpose of providing service support and IT facility management (monitoring and supporting data centers and maintaining equipment); providing software engineering, software maintenance, systems maintenance, including managing the availability, latency, scalability and efficiency of Google services; and providing customer outreach and support.

[201] The board provided a link to information about Google's affiliates who may be involved in the processing of data. The linked page advised that Google and its affiliates use a range of sub processors and listed the sub processors.

[202] In my view, any affiliates, employees, and agents should be permitted to use the information for the above-noted purposes if they have agreed to comply with the terms of the Agreement applicable to Google, including the Security Standards set out in the Attachment.

[203] I note that Item 4 of the Addendum addresses only use of, and access to, Customer Data, and does not address collection or disclosure of such information. However, I am satisfied that read together, Item 4 of the Addendum and Section 5.1 of

the Agreement provide protections for the collection, use, and disclosure of the personal information included in the Customer Data.

Confidential Information:

[204] As noted above, section 5.1 of the Agreement includes protections for Confidential Information, and imposes limits on its use and disclosure. The Addendum defines Confidential Information as information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is defined in the Addendum (replacing the definition in the Agreement), to mean data, including email, provided, generated, transmitted, displayed or stored via the Services by the Customer or End Users. The Addendum states that Customer Data is considered Confidential Information.

[205] While these provisions do not explicitly address personal information, as defined under the *Act*, I am satisfied that the contractual relationship provides protections for Confidential Information, and that the personal information belonging to students of the board is included within these protections, as part of the Customer Data.

Notice of Compelled Disclosure:

[206] Section 5.3 of the Agreement is titled Required Disclosure, and reads as follows:

> Each party may disclose the other party's Confidential Information
>
> when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.

[207] I am satisfied that section 5.3 provides protections for personal information, while also allowing for disclosure of personal information when this disclosure is required by law. However, it is important to ensure that Google remains cognizant of its obligation to report instances of compelled disclosure to the board, and that such reporting should happen prior to any compelled disclosure, when legally permissible. Accordingly, I recommend that the board follow up with Google and remind it of its obligations under section 5.3 of the Agreement.

Subcontracting:

[208] The Agreement does not use the term "subcontracting," but it appears that section 5.1, which refers to "affiliates, employees and agents", is broad enough to encompass subcontracting.

Security:

[209] The security measures in the contractual relationship include security standards, as well as notice requirements in the event of a security breach. I will address each of

these in turn.

[210] Item 7 of the Addendum states as follows:

> As of the Effective Date, Google abides by the security standards in Attachments A ("Security Standards"). During the term of the Agreement, the Security Standards may change but Google agrees that any such change shall not cause a material degradation in the security of the Services.

[211] The Attachment describes the Security Standards that apply to Google's services. These standards form part of the contract. They address the physical and electronic security precautions taken at the Google data centres located throughout the world; the methods used to protect data transmission and data networks, including intrusion detection; and access and site controls. Google's security program, and all the physical, technical and administrative controls put in place to fulfill these Standards are subject to regular, independent audits and certifications according to recognized international standards. Google must also notify the board of any security breaches.

[212] The complainant states that these security standards are inadequate, especially as they relate to encryption. The complainant states that the ISO 27001 standard[15] that Google has committed to in the Agreement does not do enough to ensure the security of the personal information held by Google.

[213] I acknowledge that the complainant believes the board should have put in place additional encryption and other security protections. However, the protections currently in place provide considerable assurances that the board is meeting its information security commitments under *MFIPPA*. ISO/IEC 27001 certification imposes extensive documentation requirements detailing how the organization is addressing all the information security control objectives, including use of encryption. The ISO/IEC 27001 standard is supported by a family of 27000 series standards that provide guidance on interpreting and meeting the implementation requirements of ISO/IEC 27001:2013.

[214] A recent report from this office also supports this view. Privacy Complaint Report MC18-48 similarly involved a cloud-based system storing student personal information. In that report, Investigator Lucy Costa recommended that the school board at issue implement security controls that aligned with "a generally accepted technical or organizational framework or standard" and provided ISO/IEC 27001 as an example.[16]

[215] Given the above, I am satisfied that the contractual arrangement between the board and Google contains provisions that protect Customer Data in Google's custody from unauthorized collection, use, and disclosure.

---

[15] This ISO/IEC 27001 standard is addressed in more detail in the Audit section of this Report, at paragraphs 241-243.

[16] See Recommendation 4 in Privacy Complaint Report MC18-48.

[216] However, that only partially addresses the security of student data within G Suite, as it only addresses the steps Google is taking. The board also has a responsibility to address security concerns regarding the information it deals with directly, in the delivery of the G Suite services.

[217] The board is using G Suite services to help deliver its education services, and as such, has to integrate G Suite into its IT infrastructure. The board has direct control over student data independent of its G Suite agreement with Google. This is evident from many of the services it provides and how it chooses to provide them.

[218] The board fully controls components of the network that interact with the G Suite service, such as student directory systems and the login portal. The board also has control of portions of the G Suite services, including the discretion to set up, configure and manage user accounts and groups, applications and service device settings, and system settings. For example, the board gets to choose the default privacy settings within applications.

[219] Consequently, the board's security policies, procedures and controls are also relevant to an assessment of whether it has reasonable measures in place to ensure the privacy and security of the personal information of its students using the G Suite services.

[220] I have reviewed all security-related documentation and representations provided by the board, as well as those available online on the board's website. This includes the Acceptable Use of Information Technology Resources Policy, which sets out rules for users of the board's information technology resources, and urges caution in using these resources.

[221] In 2019, the board implemented the Cyber Risk and Security Operations Procedure. This requires that the board perform a cyber risk assessment at the start of every digital initiative, so such risks can be managed proactively. That same year, the board enacted its Freedom of Information and Protection of Privacy Policy. This policy includes a requirement that the board establish, maintain, and continuously improve its processes relating to the collection, use, retention, and disclosure of information in its control, and in the control of its third party providers.

[222] I am generally satisfied with the adequacy of these safeguards, but I must also address the complainant's allegation that the board failed to carry out effective reviews or maintain effective oversight over Google's security policies, procedures and controls since engaging Google's services in August 2011. The complainant believes that the board conducted an initial review of the security measures but that there has been no ongoing review by the board of Google's security measures. The complainant believes that the board should be conducting ongoing reviews due to evolving law and policy considerations.

[223] The board noted that a privacy and security assessment was completed in September 2013. The board advised that it is satisfied with this assessment, and has not

completed any subsequent assessments.

[224] The board also advised that Google maintains certifications for the Core Services that are independently verified every eighteen months, as well as audit reports that are also updated every eighteen months.[17]

[225] I am satisfied that the board has exercised a minimum of due diligence when engaging Google for contracted services. Under the circumstances, I am also satisfied that the board's reliance upon periodic independent security audits and certifications is reasonable absent a real or suspected security breach.

[226] Consequently, it appears that the organizational safeguards, including physical, technical and administrative controls, are adequate, and that the confidentiality, integrity or availability of students' personal information is not compromised or threatened.

[227] I acknowledge the complainant's observation that the board has not completed any privacy and security assessments of the Google service since the beginning of the engagement. The board has a duty to monitor, on an on-going basis, significant changes which may create new privacy risks and trigger a need to update its original assessment. Given the passage of time, I will recommend that the board review whether there have been any developments in the scope of the services or their features, such that an updated privacy and security assessment is warranted. I will ask the board to provide me with the results of this review.

[228] The second category of security measures addresses the notice to be provided in the event of a security breach. This is set out in Section 2(d) of Attachment A, which requires Google to notify the school board of security breaches:

> To the extent a state or federal security breach law applies to a Security Breach, Google will comply with the applicable law. To the extent that no such law applies to a Security Breach, Google will notify Customer of a Security Breach, following the discovery or notification of such Security Breach, in the most expedient time possible under the circumstances, without unreasonable delay, consistent with the legitimate needs of applicable law enforcement, and after taking any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Google will send any applicable notifications regarding a Security Breach to the Notification Email Address or via direct communication with the Customer (e.g. phone call, in person meeting, etc.). For the purposes of this Section, "Security Breach" means an actual

[17] The board stated that Google is certified to ISO 27001, 27017, 27018 and AICPA SOC (1, 2, and 3) standards. ISO 27001 certification reports are available for inspection by the board and independently verified every 18 months. The Independent R 16/ISAE 3402 Type II DOC 2 audit report (or comparable) are also available for inspection by the board and also updated every 18 months. These certification reports and audit reports are discussed further at paragraphs 248-250 of this Report.

> disclosure, or reasonable belief that there has been a disclosure, by Google of Customer Data to any unauthorized person or entity.

Cross Border Transfers:

[229] Section 1.2 of the Agreement states as follows:

> As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data.

[230] The complainant raised concerns about students' personal information being stored outside of Canadian jurisdictions. He is particularly concerned about the personal information kept in the United States. The complainant believes that storing the data on cloud servers outside of Canada could result in the US government and its agencies accessing student information.

[231] The complainant advised that parents raised these concerns at school advisory meetings, and that the school board acknowledged that such access may be possible under the laws of those jurisdictions.

[232] The complainant believes that this compromises the students' sense of well-being and safety. He noted that students do not know if the US government is viewing their information and may choose not to explore an issue, especially a political one, if they fear that certain keywords may be captured in an electronic sweep conducted by a US government agency.

[233] It is the complainant's position that the board has essentially confirmed that they are not in control of data that is stored in foreign jurisdictions and do not have any intention of putting procedures in place to handle concerns about foreign access to students' data. The complainant believes that the board's position conflicts with its responsibility towards student safety and well-being under the *Education Act*, and that its public statements confirm that it has violated its obligations to keep records secure and prevent unauthorized access, as set out in sections 2(1) and 3(1) of *Ontario Regulation* 823.

[234] The board is of the view that the *Act* neither restricts it from storing personal information outside of Canada nor requires notice of the storage location.

[235] A previous special investigation report by this office addressed concerns about personal information being subject to and accessible under laws of the US. In Privacy Investigation Report PC12-39, former Commissioner Ann Cavoukian set out the existing Ontario requirements as follows:

> It is important to remember that, in Ontario, there is no legislative prohibition against the storing of personal information outside of the province or Canada. In other words, Ontario law, including the *Act*, does not speak to this issue. However, the *Act* and its regulations do require provincial institutions to ensure that reasonable measures are in place to protect the privacy and security of their records containing personal information. This applies regardless of where the records are located. Further, Ontario provincial institutions remain accountable for the actions of their agents or service providers, whether located in Ontario or in other jurisdictions.

[236] I agree with the reasoning of former Commissioner Cavoukian and apply it here. The *Act* does not prohibit the board from outsourcing services on the basis that a foreign law may apply and does not prohibit the storage of personal information by institutions outside the province. As outlined in Privacy Investigation Report PC12-39, the critical question is whether the institution has taken reasonable steps by way of contractual terms to protect the privacy and security of the records in their custody and control.

[237] I have reviewed those terms in my analysis above. While I make some recommendations to strengthen the board's oversight, I find that the board has reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students using the G Suite services.

[238] Although I acknowledge the sensitivity of the information at issue, I also recognize the reality that utilizing servers throughout the world is increasingly the norm for data storage and processing. A recommendation that all personal information be kept within Canadian borders would be a significant limitation to the board's options for contracting with service providers. Such a recommendation would not be made unless it was clear that the other terms were insufficient to ensure the security of students' personal information. As discussed above, that it is not the case here.

Retention and Destruction:

[239] As outlined and explained in detail under Issue 6, the complainant raised concerns that Google is not required to destroy or dispose of students' personal information and neither the Agreement or the Privacy Notice make a clear statement regarding the deletion of personal information.

[240] Under Issue 6, I have set out a detailed analysis of issues connected with the retention and destruction of students' personal information. As noted previously, I find that the contractual arrangements in place require deletion of data within a commercially reasonable time of 180 days.

Audits:

[241] Google's audit commitments are found in section 2(c) of the Attachment, which

reads as follows:

> Audits and Certifications. During the Term, Google will maintain its Standard for Attestation Engagement No. 16 audit report or a comparable report ("Audit Report") and its ISO/IEC 27001:2005 Certification or a comparable certification ("ISO Certification") for Google Apps Core Services. Google will update the Audit Report, at least every eighteen (18) months.

[242] Audits are another necessary and important way to ensure adequate oversight and compliance with the institution's obligations.[18] 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.[19] As such, I requested that the board explain the type of audits that are completed every eighteen months.

[243] In response, the board advised that Google maintains the following certifications for the Core Services: ISO 27001, 27017, 27018 and AICPA SOC (1, 2 and 3) reports. While the board's response does not itself provide details on the type of audits that are run every eighteen months, Google has made information about these certifications and attestations publicly available.[20] Both the ISO and SOC standards referred to are rigorous and recognized international standards, and the SOC 2 and 3 reports are themselves audit reports. Given this, it appears that the audits themselves are sufficient to ensure adequate oversight and compliance.

[244] However, it is not clear that the results of these audits are communicated to the board on a regular basis. It is not sufficient that regular audits be conducted to ensure the standards are being met; the information from these audits should also be communicated to the board. In this way, the board can be both kept current to any changes in compliance and understand the significance of such changes, if they do take place. Given this, I recommend that the board request that Google provide the board with regular security briefings and evidence of compliance with the audit commitments.

Governing Law:

[245] The Addendum states that the board is subject to the *Act* and is responsible for evaluating whether the use of the service is consistent with its legal obligations under the *Act*.

[246] The Agreement sets out that if the board is a "city or state government entity" within the meaning of the Agreement, then the parties have agreed to remain silent regarding governing law. However, if it is not, the governing law is California law and any

---

[18] PR16-40, page 36, para. 116.
[19] Ibid.
[20] For example, such information can be found in the Google Cloud Security and Compliance Whitepaper, found at https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf.

dispute arising out of or relating to the agreement, the parties consent to the jurisdiction and exclusive venue in Santa Clara, California.

[247] I find that the board is a "city or state government entity". It is a provincial corporation, funded by the province, and plays a significant role within the City of Toronto. Given this, I find that the governing law of the Agreement would be that of Ontario.

[248] Moreover, the Addendum clearly states that the board remains subject to the *Act*. As noted in PR16-40, an institution "must take all reasonable and appropriate measures to ensure that the [third party] entity deals with the records under the control of the institution in ways that comply with the institution's obligations under the *Act*." This obligation remains in place irrespective of the governing law of the Agreement.

Conclusion regarding the Contractual and Oversight Measures in Place

[249] Overall, I find that the board has reasonable contractual and oversight measures in place to ensure the privacy and security of the personal information of its students. However, I have made some recommendations to strengthen its oversight of those measures.

CONCLUSION:

1. The student's name, school name, email address, telephone number, and photograph 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 board's use of the information at issue was in compliance with section 31 of the *Act*.

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

5. The board has reasonable contractual and oversight measures in place regarding the retention and destruction of the personal information of its students.

6. The board has 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 its current notice of collection as it has proposed, so that it includes a reference to the authority for the collection of the personal information collected by Google on the board's behalf.

2. The board should include a copy of the revised online privacy notice, found on the Digital Learning Tools section of its website, within students' registration packages.

3. The board should reiterate to Google its obligation to provide notice of any compelled disclosure to the board, and to provide this notice prior to any compelled disclosure when legally permissible.

4. The board should request that Google provide the board with regular security briefings and evidence of compliance with the security audit and certification commitments found in the Attachment.

5. The board should review whether there have been any significant developments in the scope of the services or their features, determine whether an updated privacy and security assessment is warranted, and provide me with the results of this review.

The board has reviewed this Report and agreed to implement the above recommendations. Accordingly, within six months of receiving this Report, the board should provide this office with proof of compliance with these recommendations.

Original Signed by: July 23, 2021

Jennifer Olijnyk
Investigator