Information and Privacy Commissioner,
Ontario, Canada

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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT MC18-48

York Region District School Board

April 13, 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 York Region District School Board (the board) objecting to the board's implementation of a cloud-based data management service (Edsby), under contract with Corefour Inc. (Corefour), to store and process information pertaining to the attendance of the board's students. The complainant alleged that the board's use of Edsby contravened the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA* or the *Act*). The complainant's concerns included the board's failure to secure parental consent to the use of Edsby, the adequacy of its notice of collection, potential misuse of information by Edsby service providers, the adequacy and enforceability of the terms of the board's contract with Corefour and the adequacy of the board's oversight in relation to various Edsby security measures. The complainant also raised concerns relating to the Edsby Terms of Use and Privacy Policy and a specific security vulnerability that was exploited by the complainant.

This report concludes that the board's collection, notice of collection, use and disclosure of the students' personal information were in compliance with the *Act.* This report also concludes that the board has reasonable contractual measures in place to ensure the privacy and security of the personal information of its students.

However, this report concludes that the board has not demonstrated that it has reasonable oversight measures in place in relation to the performance of the board's and Corefour's contractual security obligations, in accordance with the requirements of the *Act* and its regulations. In particular, the board did not have reasonable measures in place to prevent the security vulnerability that was exploited.

This report makes recommendations as to the steps the board should take to strengthen and document the board's oversight of security measures. This report also make recommendations with respect to its contract with Corefour and the Edsby Terms of Use and Privacy Policy.

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; *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A.

Orders and Investigation Reports Considered: Privacy Investigation Report PC12-39; Privacy Complaint Report PR16-40; *Public Service Commission (Re)*, 2013 CanLII 55439 (SK IPC); Investigation Report IR19-01, *Department of Internal Services (Re)*, 2019 NSOIPC 2 (CanLII).

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

SUMMARY OF COMPLAINT:

[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* (the *Act*) relating to the collection, use and disclosure of the complainant's child's personal information by the York Region District School Board (the board).

[2] By way of background, the board is a public district school board, responsible for providing education services to approximately 125,000 English public elementary and secondary school students residing in York Region.

[3] In order to manage registration and attendance information, the board uses a cloud-based storage and data management service called Edsby which is owned and operated by CoreFour Inc. (CoreFour). The board retained CoreFour under an agreement to provide services in relation to the board's information management services functions, including attendance keeping functions. The personal information held by the Edsby platform at issue in this complaint relates to that function.

[4] The complainant is a parent of a child who attends a school of the board. The complainant's concerns are related to the board's implementation of Edsby to store and process information pertaining to the attendance of the board's students. Although the complaint was filed by the child's mother, the child's father also communicated with the IPC and provided information at various times in this investigation. Since they evidently share a common interest, this report refers to the parents interchangeably.

[5] The complainant states that in and around November 2017, the board advised parents that it would be using an online cloud-based system to store and share student information with parents on a third-party platform called Edsby for attendance reporting purposes, as well as to register for parent-teacher interviews. Parents were sent login information by email from Edsby inviting them to create an account and log in to its

system. When the complainant logged in to Edsby, the account was prepopulated with his child's data. The information included his child's name, grade, teacher and a picture of his child. The complainant states that he was not asked for permission to share his children's data with Edsby.

[6] The complainant advises that he contacted the school to request that his information and his child's information be removed from the Edsby platform. His request was denied. The complainant was also told by the board that his consent was not required for the purpose of taking attendance and only minimal information about his children would be tracked.

[7] In his complaint, the complainant also raised concerns about Edsby's privacy policy, which he believed allowed Edsby to share information with parent companies, affiliates and third parties, as well as sell student information. The complainant alleges that the board's selection process for the third party supplier failed to address aspects of security or privacy and was therefore flawed.

[8] The complainant also alleges that the personal information provided to Edsby is used for purposes beyond attendance, such as for data aggregation including the collection of location data, school reports, assignments, instant messaging, scheduling, academic performances, report card information and copying and storing documents from other platforms.

[9] The complainant further alleges that the Edsby platform contains security vulnerabilities. In January 2019, he notified the board of a security vulnerability within the Edsby platform which allowed him to access students' profile pictures. The complainant provided four photos to the principal of his child's school and advised that he had the consent of the parents of the four students to use their child's images. The complainant believes that the Board should notify all parents in its system of this security vulnerability.

[10] The complainant also alleges that Edsby does not have security or privacy personnel with sufficient expertise to ensure adequate software testing and quality control.

[11] Generally, the complainant maintains that personal information of parents and students should never be shared with a third party without the express consent of the parent and/or student and that all data already shared should be removed permanently from the third party systems and the systems of their affiliates.

[12] Further, the complainant believes that students' personal information should not be stored in a cloud-based system, in that this type of information is a prime target for hackers, child predators and ransomware attempts. He alleges that the board has failed to explain to parents the risks of storing personal information in the cloud. The complainant believes that the board should have required parental consent prior to "sharing" the complainant's children's data with Edsby and that parents should have the

right to opt-out of using this platform.

INVESTIGATION:

[13] The IPC requested that the board address the complainant's allegations as well as detailed questions concerning the Board's use of the Edsby platform, and its contractual and other oversight of the security of this platform.

[14] The board disputes the complainant's various allegations and, more specifically, the claims: (1) that parental consent is required in the circumstances of this case; (2) that the personal information collected and used employing the Edsby platform is not sufficiently secure; and (3) that the board did not engage in appropriate processes to evaluate the security of the platform. It provided the IPC with a copy of the "Service Provider Privacy and Security Assessment Tool" used to evaluate the product. The board also advises that it engaged the services of a third party to conduct an assessment of the Edsby application,[1] which concluded that the Edsby solution provided appropriate security and privacy controls for the student data it managed.

[15] The board's submissions in response to the issues raised by this complaint are set out under the corresponding issue headings below.

[16] The complainant was provided with a summary of the board's submissions and made lengthy submissions in response. The complainant raises particular concerns in several related areas: the role of parental consent, the scope of personal information affected by the new system, the potential expansion of Edsby beyond the attendance monitoring function, the qualifications of Corefour's management and staff, Corefour's use of unknown third party service providers, potential security vulnerabilities of web-based platforms handling personal information, including specific vulnerabilities in the Edsby system. He raised questions about the financial costs of the system, the ethics of the board's decisions, and the motives and credibility of the board and its management team. The complainant also disputes the adequacy of the board's past and current contractual arrangements with Corefour, points to apparent conflicts between those contracts and Corefour's published policies, and questions the board's ability to effectively oversee and enforce Corefour's obligations in relation to various security measures. Many of the complainant's submissions extended well beyond the scope of the *Act*.

[17] I do not intend to address all of the complainant's submissions in this report. The role of this office in investigating privacy complaints is to determine whether the institution is in compliance with the provisions of the *Act*, which requires that I address

---

[1] Assessment of Hosted Edsby Portal Application, Digital Defense Inc, February 2018.

the issues set out below. It is not my role to rule or comment on the wisdom or cost-effectiveness of an institution's business model, procurement processes or choice of vendors in introducing a new information management system into its operations. It is also beyond the scope of this report to make any findings on potential expansions to the services. My role is to determine whether the board's arrangements with Corefour in deploying the Edsby system to monitor the attendance function complies with the board's obligations under the *Act*, and this report focuses on this essential question.

[18] Finally, I note that the board was provided with a copy of the complainant's submissions and was invited to respond to them.

ISSUES:

[19] This report deals with 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 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 THE INVESTIGATION:

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

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

> Personal information means recorded information about an identifiable individual, including,

> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> (e) the personal opinions or views of the individual except if they relate to another individual,
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and
>
> (h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

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

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

[23] The information at issue in this complaint includes the child's name, grade, teacher, picture of the complainant's child, contact information such as phone numbers

---

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

or email addresses, information identifying the complainant and the child's attendance information. This information is linked to the complainant's account information and is accessible to the complainant via the account for purposes of reporting attendance information to the child's school.

[24] There is no dispute, and I find, that the information at issue is personal information within the meaning of section 2(1) of the *Act*.

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

[25] Section 28(2) of the *Act states:*

> Collection of Personal Information
>
> > 28(2) 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.

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

[27] In order for a given collection of personal information to be permissible under the *Act*, the institution in question must demonstrate that the collection was in accordance with at least one of the above noted conditions. In this investigation, the board has advised that collection of the personal information in question is necessary to the administration of a lawfully authorized activity.

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

> ...[T]he 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.[4]

[29] 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.

Board's representations:

[30] The board explains that it collects the personal information of parents and their minor children directly upon registration and while the student attends school. This collection includes the student's name, address, contact information for the student's parent/guardian, and age, among other information, all of which the board states is necessary to provide educational programming and services to students who are compelled by the *Education Act* to attend school. The board advises that it collects the personal information of the parents of students for the purpose of communicating home in case of an emergency, absence reporting by the parent to the school, booking appointments for Parent/Teacher interviews, and daily attendance. This information is used to provide services and support to students and their families.

[31] The board states that this personal information is necessary to verify the registration of students in compliance with section 21 of the *Education Act*, which requires mandatory school attendance of children ages 6 through 18 years of age. The board explains that a parent may be charged under the *Provincial Offenses Act* for the failure of his/her child to attend school and the court may fine the parent if convicted. Further, the board is required to use the personal information to ensure compliance with the mandatory attendance reporting provisions set out in section 28(1) of the *Education Act*. In addition, the board points to its duty under section 170(1)15 of the *Education Act* to report the non-enrolment of school age children to the Ministry and the duty of principals under 265(1)(c) to register pupils and record their attendance.

[32] The board observes that the authority in the *Education Act* for the collection of personal information for attendance purposes is also mandated by the Ministry of Education's Enrollment Register Instructions for *Elementary and Secondary Students, 2018-2019* and the Policy Program Memorandum 123 Safe Arrivals. The board is required to implement a safe arrival process that requires, among other things, that the board notify parents, or an alternative individual for whom consent has been provided by the parent, in the event that the parent's child has not arrived at school and no absence of that child has been reported. The board's responsibilities in this connection are identified in both the Ministry's *Policy Program Memoranda 123 Safe Arrivals* and the board's own policy.

---

[4] *Cash Converters Canada Inc. v. Oshawa (City)*, 2007 ONCA 502, paragraph 40.

[33] On this basis, the board submits that the collection of all of the personal information at issue is authorized under, and in compliance, with section 28(2) of the *Act* as necessary to the proper administration of a lawfully authorized activity. The board states that it is not required to obtain consent for the collection of the personal information of the complainant and her child for the purpose of attendance monitoring as it is necessary to fulfil the board's statutory duties and comply with the directives of the Ministry of Education in that connection, all in aid of providing education services to students who are compelled by the *Education Act* to attend school.

Complainant's representations:

[34] The complainant agrees that the collection of the personal information at issue is necessary and that the board's submissions regarding its statutory obligations in this connection are "both correct and indisputable." The complainant's position is, rather, that the board requires parental consent to collect this information through the Edsby platform. The complainant cites no statutory or other authority for any additional consent requirement flowing from the board's use of a service provider's web-based information management system. The complainant's position in this respect is reflected in the following statement:

> Based on our understanding, parental consent is required by MFIPPA in cases where the new system is significantly different from the old. Even though MFIPPA is inadequately positioned to cover such vast leaps in business model and technology, it is clear that the original attendance process – a mere sheet of paper that preserved chain of custody as it was physically handed to a trusted office clerk - was designed to reliably allow the school to record the presence of students in their respective classes.
>
> The new system is fundamentally different. It is a website that requires student files to be first uploaded to the Internet so that each day, students are matched to their digital files in the custody of a local company that designed its cloud interface.

Finding

[35] It is not disputed, and I find that the board has the authority to collect the personal information of the complainant and the complainant's child at issue in this complaint in connection with the provision of education services. Specifically, the authority is based on the requirement to fulfill both its statutory responsibilities and its duties to implement the directives of the Ministry in recording, monitoring and reporting on school attendance. In short, the collection of this information is necessary for the proper administration of the board's lawfully authorized activities within the meaning of section 28(2) of the *Act*. The *Act* does not establish any requirement for consent to the collection of personal information in these circumstances and I confirm that the consent of the complainant was not required in this case.

[36] The complainant's submission that consent is required for the board to use Edsby to collect this information is addressed below, in my discussion of the board's authority to retain a service provider to perform this function.

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

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

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

Board's representations:

[38] The board advises that it provides notice of collection to parents pursuant to and in compliance with section 29(2) of the *Act*. The board explains that parents/families are notified of the board's collection, use and disclosure of student information in the School Start-up Package that is shared annually with all families, and in the Privacy and Information Management statement that is posted on the board's public website.

[39] The personal information at issue is derived primarily from the board's student registration information form, a copy of which the board has provided and which contains the following statements:

> Information on this form will be used for home/school communications, planning and programming such as transportation, and to establish the Ontario Student Record.
>
> ....
>
> Personal information is collected at registration pursuant to the Education Act and the *Municipal Freedom of Information and Protection of Privacy Act*. Questions about the collection and use of this personal information should be directed to the Privacy Office, York Region District School Board, 60 Wellington Street West, Box 40, Ontario L4G 3H2 or (905) 727-3143, Extension 2015.

[40] The board also provided a copy of its posted Privacy and Information Management Statement containing a notice of collection and describing the purposes for which personal information may be used, retained or disclosed in accordance with the *Act*, the *Education Act* and other applicable legislation.

[41] The board explains that it provided notice to parents advising that the Edsby digital platform would be used by the board to facilitate student attendance monitoring. The board provided a one-page handout titled "Welcome to Edsby" advising parents that it has partnered with Edsby to provide a secure platform for families to connect with what is happening at school and with their child's education. The handout identifies features that the board will be rolling out over the next few years and includes information about setting up the Edsby account for the first time. The handout advises that Edsby contains personal information of students and their parents collected by the board at the time of registration which is used to provide services and support.

[42] The board also provided a subsequent handout titled "Introducing Online Absence Reporting". This handout advises parents that absences can now be reported online though their Edsby account, discusses the importance of reporting absences and states that families can still continue to report absences by phone. The board advises that parents received these notices from their schools at the launch of online absence reporting. In addition, the board states that information regarding Edsby and safe arrivals is available on its website, which includes on-line instructions for parents. Further, parents are informed that they may speak to their school principal in the event that they have questions regarding the board's processes.

Complainant's representations

[43] The complainant does not dispute the board provided notice of collection but appears to claim the notice was inadequate for several reasons, including that the handout:

i. does not inform parents of the full list of parties that have access to all the content data, metadata and other derived information such as logs, transactions, location and behavioural information, which are the types of data that are typically monetized by the types of partners that the Vendor has selected;

ii. fails to mention the complex ways in which the data can be repurposed and analyzed to the detriment of students;

iii. wrongly claims that Edsby is a secure platform; and

iv. invites parents to voluntarily enter medical reasons for absence and clinical details.

Finding

[44] The complainant's submissions do not address the adequacy of the board's notice of collection within the meaning of section 29(2). That provision requires the board to inform the complainant of the legal authority for the collection and the principal purpose or purposes for which the personal information is intended to be used. As will be discussed below, the matters he raises are highly speculative and not based in the evidence, and in any event, are not relevant to whether the board's notice meets the requirements of section 29(2).

[45] The documentation provided by the board and referred to above demonstrates that the board has provided ample notice of collection of the personal information used for attendance purposes, including in connection with the Edsby online absence reporting platform, in compliance with section 29(2) of the *Act*.

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

[46] 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*.

[47] The meaning to be ascribed to "consistent purpose" under section 31(b), as well under section 32(c) relating to permissible disclosures, is set out at section 33 of the *Act*, 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.

Board's representations:

[48] The board advises that, by virtue of section 31(1)(b) of the *Act*, it is not required to seek consent from parents to use the personal information collected for attendance monitoring. The board reiterates that it has the statutory power and duty to monitor,

record and report student attendance as one of its core functions and that the content of the information at issue relates directly to that function. The board explains that it uses the personal information for the purpose for which it was obtained and compiled, specifically recording, monitoring and reporting attendance which is authorized by, and is an express duty of school principals under the *Education Act*. The board explains that the use of personal information for this purpose is also mandated by the Ministry of Education's Enrollment Register instructions for *Elementary and Secondary Students*, 2018-2019, as well as in connection with the safe arrivals programs described above.

[49] Given its statutory duties under the *Education Act* and the Ministry's directives for monitoring student attendance, the board submits that parents would reasonably expect such a use of the personal information as a "consistent purpose" in compliance with section 31(b) of the *Act*.

Complainant's representations:

[50] The complainant again states that she does not dispute the board's authority to collect the information at issue for attendance monitoring, but rather disputes "the decision to vastly increase the risk of doing so by unnecessarily complicating the process, introducing many other parties, unknown service providers and the very real potential that the information will be misused for any other purposes unrelated to attendance." She claims that the board's assumption that parents would reasonably expect the use of the information as a "consistent purpose" effectively misrepresents "the nature of the system, whose purpose is to collect and use the data and [place] it in the custody of other parties." Further, she claims that parents "would have no reason to believe that the traditional attendance process has any consistency with the cloud-based process ... that aggregates all attendance information for all students for the entire region" making it a target for "cybercriminals, whose business models thrive on the exploitation of data aggregators, especially those in the same situation as this Vendor."

Finding

[51] I agree with the board's submission that use of the personal information at issue for attendance monitoring and recording purposes is in compliance with section 31(b) of the *Act*. More specifically, I conclude not only that parents in the position of the complainant would reasonably expect such a use, but also that the use of the personal information for attendance monitoring purposes falls squarely within the ambit of "home/school communications" and "establish[ing] the Ontario Student Record," as purposes for which it was originally obtained or compiled.

[52] The complainant's submission that parents would not reasonably expect the board to use a cloud-based platform to assist in the attendance monitoring function speaks to the means the board has employed to perform that function but does not detract from the "use" of the information for the purpose for which it was collected or for a consistent purpose. Again, this submission is more appropriately considered in my

examination of the security measures in place, as discussed later in this report.

[53] I note that the board also takes the position that the transfer of the personal information to Edsby for the purposes set out above is a "use" of personal information within the meaning of section 31 of the *Act*. I disagree. Under the *Act*, transfers of personal information from an institution to its officers, employees, consultants or agents are all treated as "disclosures", even where they are done in the course of mandated activities on behalf of the institution (see my discussion below). In this respect, the definitions of "uses" and "disclosures" under the *Act* may differ from other legislation in which such transfers are treated as "uses" rather than "disclosures."[5] In itself, this does not signal a difference in the approach to when such uses or disclosures are permitted. At the end of the day, as set out more fully below, the transfer of personal information from the board to Edsby, like a transfer from the board to its own employees, is a disclosure which must be authorized under one of the parts in section 32 of the *Act*.

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

[54] Personal information in the custody or under the control of an institution cannot be disclosed except in the specific circumstances outlined in section 32 of the *Act*. The relevant parts of that section read as follows:

> An institution shall not disclose personal information in its custody or under its control except,
>
> > (c) for the purpose for which it was obtained or compiled or for a consistent purpose;
> >
> > (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;

Board's representations:

[55] In the previous section, I rejected the board's claim that the transfer of students' personal information from the board to Edsby constitutes a "use" of the information by

---

[5] See Ontario's *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A. for instance, in which transfers of information from a health information custodian to its agents are treated as "uses" rather than "disclosures". This is also different from the interpretation of the Saskatchewan Information and Privacy Commissioner in the decision cited by the board, in which the Saskatchewan IPC treats the transfer of personal information by a public body to its agents as a "use": *Public Service Commission (Re)*, 2013 CanLII 55439 (SK IPC).

the board pursuant to section 31(b) of the *Act*. In the alternative, the board submits that the disclosure is made in accordance with section 32(c) and/or section 32(d) of the *Act*.

[56] The board submits that the disclosure of personal information from the board to CoreFour is for a purpose consistent with the reason that it was compiled in accordance with section 32(c), namely, data management for compliance with the board's duties under the *Education Act* and the Ontario Ministry of Education's *Safe Arrival* and Attendance Register guidelines regarding attendance monitoring and reporting. Further, the board submits that performance of these data management functions by CoreFour on behalf of the board would be reasonably expected by the complainant and other parents as they are solely related to the board's purposes, and they are functions which were explicitly communicated to parents, including the complainant, as described above.

[57] In addition, or in the alternative, the board submits that the personal information collected by the board is disclosed to CoreFour as an agent and that this disclosure is in accordance with section 32(d) of the *Act*. The board states that CoreFour requires the data for the purpose of fulfilling its contractual obligations to the board to support the discharge of the board's functions as they relate to attendance monitoring and reporting pursuant to the *Education Act* and the Ministry's Safe Arrival's policy and Attendance Register guidelines.

Complainant's representations:

[58] The complainant agrees that, when acting with due diligence, the board can engage any third party it wishes without notifying parents. In the circumstances of this case, however, the complainant submits that the board should have notified parents, explained the impact of the transfer of information and sought explicit, informed consent from parents and guardians. Further, the complainant submits that the board had a duty to act ethically "beyond legal requirements" in view of the fact that the *Act* was written before cloud-based technologies existed.

[59] She submits that the "consistent purpose" provision at section 32(c) of the *Act* does not give the board authority to disclose personal information because the purpose of taking attendance manually is different from the purpose of collecting it on a computer where it can be accessed and used by Corefour's partners, contractors and service providers and used for other purposes. Further, she submits that section 32(c) does not apply because parents would not reasonably expect processing would be performed by a private vendor and its partners when another system adopted by several other school boards is available.

[60] The complainant submits that the "agency" provision at section 32(d) does not authorize disclosure because, while the board remains legally responsible for the information, it has effectively relinquished control over the data to an extent that Corefour cannot be held accountable as an agent of the board. Further, she submits

that the board itself cannot be held accountable because it is not in a position to monitor the data in the same way as if it had remained in its own servers. At the same time, she appears to suggest that disclosure to an agent on a cloud-based system would be appropriate if it was less costly and risky than it is in this case. The complainant's submissions on this subject go on to suggest that the board's arrangements with Corefour shield it from responsibility for notifying data subjects about privacy incidents and facilitate the misuse and monetization of students' personal information.

[61] Again, the complainant submits that the board should have sought parents' informed consent to the disclosure of the information, which would provide the necessary authorization under section 32(b) of the *Act*.

Finding

[62] At the outset, I would note that while the control and accountability considerations raised by the complainant are important, they are more appropriately examined in my discussion of the contractual and oversight measures set out below.

[63] I would also note that, in order for disclosure of the personal information at issue to be authorized, I need only be satisfied that one of the exceptions under section 32 of the *Act* has been satisfied.

[64] Section 32(d) of the *Act* explicitly recognizes the authority of institutions to engage agents to perform functions that involve the use of personal information and, in that connection, to disclose the information to persons who need it to perform those functions. This provision does not limit the circumstances in which an institution may retain an agent. For example, it does not set up a test of necessity for an institution to engage an agent, just as it does not set up a test of necessity for appointing an officer or hiring an employee or consultant. The words "necessary and proper" simply mean that the function cannot be performed properly unless the information in question is disclosed. The use of the word "needs" means that the officers, employees, consultants or agents require the information to perform their duties in relation to that function.

[65] Further, I would note that this Office has specifically recognized that, in proper circumstances cloud-based solutions to the information management functions of public institutions, including the processing personal information, can be a necessary and desirable means to accommodate ever-increasing demands for the efficient and cost-effective performance of their core mandates.[6]

[66] The board clearly has the authority to retain a third party as an agent to assist in

[6] Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions. IPCO, February 2016.

performing its information management functions, including with respect to personal information. Further, the Board may disclose personal information to an agent where, in accordance with section 32(d), the agent "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." There is no impediment in section 32(d) to the board engaging a private sector service provider as its agent to assist it in performing these functions using a cloud-based information management system. I am satisfied that the requirements of section 32(d) are met here and that the consent of parents and guardians to disclosure of the personal information at issue was not required in this case.

[67] In view of the foregoing, I find that the disclosure of the personal information at issue is in compliance with section 32(d) of the *Act*. It is not necessary for me to go on and consider whether the disclosure is also authorized under section 32(c).

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

[68] Two areas of examination are critical in addressing the reasonableness of privacy and security measures where a third party contractor is retained by an institution to perform information management functions. The first involves a determination whether the institution has and retains control over the information in the context of the specific statutory and regulatory regime in issue.[7] The second examines the presence of adequate contractual and oversight measures to ensure that the institution remains in compliance with its obligations under the *Act*.[8]

[69] The complainant appears to accept that the board has "legal control" over the personal information, but throughout her submissions relies on the fact that "the actual operational control is exclusively in the hands of Corefour."

[70] The thrust of the complainant's submissions on this issue appears to be directed at the enforceability of the contract terms and the adequacy of the board's oversight measures. I do not intend to set out the complainant's lengthy submissions in this connection. My analysis and recommendations below address these concerns to the extent they are relevant to the issue of compliance with the *Act* and regulations.

[71] I would emphasize here that my role is not to examine every alleged deficiency in the board's arrangements with Corefour at a given point in time, but rather to determine whether the board has reasonable privacy and security measures in place to protect the personal information of students and parents and to make

---

[7] *Ontario (Criminal Code Review Board) v. Doe*, 47 O.R. (3d) 201 (C.A.).
[8] *Ontario Criminal Code Review Board* (C.A.); Privacy Complaint PR16-40, *Ontario Lottery and Gaming Corp. (Re), [2019] O.I.P.C. No. 11.*

recommendations for improvement where appropriate.

The board has "control" over personal information in Edsby

[72] Although there appears to be no dispute that the personal information in the Edsby system is under the board's control at law and that the board is ultimately responsible for its security, it is useful to outline briefly the statutory and contractual bases for this conclusion. Guidance in this regard is found in the IPC's Privacy Complaint Report PR16- 40 where personal information held by a private sector company under contract to operate a casino in Ontario was found to be under the control of the Ontario Lottery and Gaming Corporation.[9] That Report lists a series of non-exhaustive factors (at paras. 51-52) to be considered when determining the control issue, including in cases where an organization other than the institution holds the record or information in issue. I will not list all of the potentially relevant factors separately here. However, it is clear from the material I have been provided that the personal information at issue is under the control of the board based on the following:

- The information was created by board staff from student registration information.
- The information is used for student registration and other board purposes including recording student attendance.
- The board has the statutory power and duty to monitor, record and report student attendance as one of its core functions.
- The content of the information at issue relates directly to that function.
- The board has the authority to regulate the content, use and disposal of the information.
- The board retained CoreFour under an agreement as an agent of the board to provide services in relation to the board's attendance keeping functions and the personal information held by Edsby relates to that function.
- The board receives and retains attendance information recorded on the Edsby system.
- A Confidentiality and Security Agreement between the board and CoreFour dated August 5, 2016 acknowledges that the personal information is under the control of the board and subject to *MFIPPA*. This agreement binds CoreFour to the following obligations:

---

[9] Privacy Complaint PR16-40; *Ontario Lottery and Gaming Corp.*, [2019] O.I.P.C. No. 11.

  - To comply with *MFIPPA* and all board polices and procedures regarding the collection, use and disclosure of the personal information.

  - To employ appropriate security measures as determined by the board and protect the confidentiality of personal information in its possession but under the board's control.

  - To permit access to the personal information only by its employees or agents who require the information to perform the duties required in relation to the services provided.

  - To return or destroy all personal information under the board's control, as determined by the board, that comes into the possession of CoreFour as a result of the services it provides to the board.

  - To indemnify the board in relation to any breach of the agreement.

- A letter of amendment to the agreement dated November 23, 2018 provides that board data shall at all times remain the sole property of the board and that CoreFour is not granted any license or other proprietary right to the board data.

- This latter agreement goes on to detail CoreFour's obligations to the board (discussed more fully below) with respect to maintaining the privacy and security of board data.

[73] I note that the 2016 Confidentiality and Security Agreement provides that personal information collected by CoreFour for its own use and benefit (i.e., not under the board's control) is subject to the application of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). However, this agreement goes on to provide that at no time will CoreFour use and/or disclose personal information about and/or belonging to students of the Board for its own use or benefit. The board maintains that neither this provision nor any other agreement between the board and CoreFour provides Edsby with any authority or consent to collect, use or disclose information for its own purposes. The board states that should Edsby desire to use any board data that is the personal information of students and/or parents/guardians for its own purposes, Edsby would require consent.

[74] On the basis of the evidence before me, the board has retained legal control over the personal information of students or their parents collected by CoreFour in the course of providing services to the board under the contract. The statutory obligations that apply to this information are therefore found in the *Act*, and not *PIPEDA*.

Are adequate contractual measures in place?

[75] Section 3(1) of Regulation 823 under the *Act* states*:*

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[76] In Privacy Complaint Report PR16-40, I stated the following regarding section 4(1) of Regulation 460 of the *Freedom of Information and Protection of Privacy Act* (which mirrors section 3(1) of Regulation 823 of the *Act*):

> 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.
>
> Furthermore, simply because a breach occurred does not by itself mean that reasonable measures were not in place. The standard set out in 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.

[77] The IPC's approach to assessing 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 under its control is set out in Privacy Complaint PR16-40[10] as follows (in part);

> 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*. Audits are another necessary and important way to ensure adequate

---

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

oversight and compliance with the institution's obligations. Implementation of audits should also be expressly provided for and made enforceable under the terms of the agreement between the institution and the private sector entity.

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).[12] 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. In this regard, the following provisions of the contract are relevant:

Ownership - The contract states that the Ministry shall be the owner of all Ministry data. Ministry data is defined in the contract to include: all data created or modified by the LAS as well as the data relating to licence issuers and angler and hunter licence records, including all data created, modified, collected and stored in the LAS database and any legacy data.

Collection, Use and Disclosure - The contract states that the Agent cannot directly or indirectly use, collect or disclose any personal information for any purposes not authorized by the Ministry. In particular, the Agent has acknowledged in the contract that unless it obtains specific, written pre-authorization from the Ministry, any access to or use of the Ministry's property, technology or information that is not necessary for the

performance of its contractual obligations with the Ministry is strictly prohibited. These restrictions would prohibit the Agent's sale of personal information without the Ministry's consent.

Confidential Information - Confidential information is defined in the contract to include all personal information that the Ministry is obliged, or has the discretion not to disclose under provincial or federal legislation or otherwise at law. The Agent's contractual obligations for this information include:

(i) keeping the information confidential and secure;

(ii) limiting the disclosure of confidential information to only those who have a need to know it for the purpose of the contract and who have been specifically authorized to receive such disclosure; and

(iii) not directly or indirectly disclosing, destroying, exploiting or using any confidential information (except for the purpose of the contract, or except if required by order of a court or tribunal), without first obtaining the written consent of the Ministry and in respect of any of the Ministry's confidential information about any third party, the written consent of such third party.

It is important to note that these restrictions would also prohibit the Agent's sale of personal information without the consent of the Ministry and relevant third party.

Notice of Compelled Disclosure - If the Agent is legally compelled to disclose any of the Ministry's confidential information, the Agent must provide the Ministry with prompt notice to allow the Ministry to seek a protective order or other appropriate remedy to prevent or limit such disclosure. Further, the Agent will disclose only that portion of the confidential information which the Agent is legally compelled to disclose.

Subcontracting - The contract states that the Agent is not permitted to subcontract the whole or any part of the contract without the prior written consent of the Ministry. If the Ministry does consent to the Agent subcontracting certain services, the Ministry may impose the same contractual obligations on the subcontractor that were imposed on the Agent.

Security - The contract states that the Agent must ensure the security and integrity of all personal information and records in its possession. The Agent must keep the personal information and records in a physically secure and separate location, safe from loss, alteration, destruction or intermingling with other records and databases. Further, it must

implement, use and maintain the most appropriate products, tools, measures and procedures to do so. The Agent has also provided the Ministry with point-of-sale devices that incorporate reliable security, including secure operating and control systems that prohibit any incoming connection to the devices.

Retention and Destruction - The contract states that the Agent must return all of the Ministry's confidential information to the Ministry before the end of the term of the contract, with no copy or portion kept by the Agent. The Ministry has also stated that it has initiated the development of a retention and destruction schedule with the Agent. The Ministry expects the retention and destruction schedule to be completed by the spring of 2013.

Audits - The contract states that the Agent will comply with annual audits for privacy and security compliance, for the duration of the contract. These audits may include reviews of threat risk assessments, Privacy Impact Assessments (PIAs) and vulnerability assessments.

Governing law - The contract clearly states that the governing law of the contract is Ontario and the federal laws of Canada.

The contract documents between the Board and CoreFour

[78] The board has provided us with the following contractual documents:

1. The board's Request for Proposal #15R523 Provision of a Cloud Based Enterprise K-12 Engagement Platform dated July 2015 ("RFP").

2. CoreFour's 144 page Proposal document dated August 6, 2015 in response to the RFP.

3. A 2 page Contract Agreement for Services between the board and CoreFour dated August 5, 2016 appended to the RFP which, together with the August 6, 2015 Proposal document, comprises the contract for the services set out in the RFP.

4. An Agreement for the Confidentiality and Security of Personal Information dated August 12, 2016 (the "Confidentiality and Security Agreement").

5. A Letter of Amendment for Contract Agreement RFP15R523 Provision of a Cloud Based Enterprise K-12 Engagement Platform entered into between the board and CoreFour dated November 23, 2018 (the "Amending Agreement").

[79] Article 8.4 of the board's RFP (at item 1 above) requires the successful vendor to complete an Agreement for the Confidentiality of Personal Information (Appendix H) and a Privacy Impact Assessment Checklist (Appendix I) prior to final award.[11] The August 12, 2016 Confidentiality and Security Agreement (at item 4 above) appears to be the agreement contemplated in Article 8.4 of the RFP. The board advises that the privacy impact assessment checklist contemplated in the RFP was not completed and has provided, in its place, a document entitled Third Party Privacy Agreements for Outsourced Services – Service Provider Privacy and Security Assessment Tool (the "Assessment Tool"), which is a form of questionnaire completed by CoreFour that is broadly equivalent. Vendor responses to the questionnaire are used by the board to evaluate the vendor's privacy and security posture for procurement decision purposes.

[80] The November 23, 2018 Amending Agreement was entered into following the initiation of this complaint and incorporates several terms and conditions recommended by an independent security expert in a report prepared for the board titled an Assessment of Hosted Edsby Portal Application dated February 20, 2018.

Independent Security Expert's Assessment of Edsby

[81] Given the general nature of the security issues raised in the complaint, it is useful to summarize briefly here the scope of the assessment conducted by the security expert and the findings and recommendations set out in the expert's report.

[82] The security expert was retained to review the security and privacy of data provided by the board for storage and processing by the Edsby application. The expert reviewed the Edsby online application, CoreFour's enterprise security practices and the contractual arrangements between CoreFour and the board.

[83] The expert tested the Edsby online application against an established security framework and evaluation criteria and concluded that "[t]he Edsby portal has sufficient controls in place [to] protect student data stored in this online system." The expert noted that "[s]ome vulnerabilities were identified in the present Edsby implementation; however it must be emphasized that none of these vulnerabilities were exploitable during penetration testing." The expert then made a number of technical recommendations to address these vulnerabilities which, as he notes in his report, CoreFour advised that it had implemented.

[84] The expert also carried out a review of CoreFour's Edsby premises, which included an assessment of the security practices that protect board data accessible by Edsby employees, including during the software development process. This review was

---

[11] RFP - 8.4 The successful vendor will be required to complete Appendix H Agreement for the Confidentiality of Personal Information and Appendix I Privacy Impact Assessment Checklist prior to final award.

conducted using an internationally accepted security standard and was based upon statements and claims made by Edsby that were not directly verified or proven by audit. The expert's report concluded that "Edsby's security practices are aligned with accepted control standards" but that there were some "opportunities for improvement."

[85] On my review, I find the security expert's report to be an accurate guidepost to the "reasonable measures" the board and its agents must take to protect personal information, as required by section 3(1) of Regulation 823. The expert made a number of recommendations to improve Edsby's organizational security practices, including specific measures to:

- implement formal security policies and practices;
- ensure physical and logical access controls;
- carry out regular vulnerability scans and penetration tests;
- monitor inappropriate or suspicious use of data;
- ensure secure coding and configuration practices; and
- extend security requirements to third party providers.

[86] While the board advises that CoreFour committed to implementing the report's recommendations, and at least some appear to be reflected in the Amending Agreement, it is not clear whether the board followed up with Corefour to confirm that each of the above-noted recommendations was, in fact, implemented. I will be recommending that the board take the necessary steps to ensure that Corefour has implemented all of these recommendations.

[87] The security expert also made recommendations intended to strengthen the contractual arrangements affecting the privacy and security of board data held and processed by CoreFour/Edsby. These included amended contractual provisions to:

- broaden and clarify the scope of the service agreement;
- require regular testing and validation of security measures in place;
- clarify the responsibilities of CoreFour and any third party vendors engaged by CoreFour;
- ensure the board's right to audit security controls in place;
- have a formal incident response plan, approved by the board; and
- notify the board in the event of any suspected or real breach of board data

[88] As noted above, CoreFour and the board implemented these contractual recommendations in the Amending Agreement dated November 23, 2018.

[89] The complainant observes that the independent security review was carried out more than three years after the initial CoreFour contract was signed and only as a result of her privacy complaint and security vulnerabilities that came to light. I draw no conclusions as to whether the privacy complaint was the impetus for the review. While I acknowledge the complainant's views, one of the purposes of this report is to make recommendations to the board regarding steps it should be taking in the future to ensure compliance with the *Act*. Where it is clear that the board has already implemented the expert's recommendations to improve security through contractual and other oversight measures, no useful purpose would be served by revisiting the basis for each of those recommendations.

Adequacy of the Contractual Terms between the Board and CoreFour

[90] My analysis of the contractual provisions between the Board and CoreFour is guided by this office's approach in Privacy Complaint Reports PC12-39 and PR16-40, referred to above. I note at the outset that the Confidentiality Agreement and the Amending Agreement, between them, contain provisions addressing virtually all of the accountability, privacy and security issues identified in those earlier reports. Gaps in the original Confidentiality and Security Agreement have largely been remedied by the additional provisions set out in the Amending Agreement, as described more fully below.

Ownership

[91] The questions of control over and ownership of the personal information at issue are satisfactorily addressed in the contract terms as follows:

- The Confidentiality and Security Agreement acknowledges that CoreFour requires access to and/or possession and/or use of personal and business information under the control of the board in connection with the services provided.

- The Confidentiality and Security Agreement provides that the *Act* and Regulations thereunder apply to the collection, use and disclosure of personal information under the control of the board and subject to the *Act*.

- The Amending Agreement provides that board data shall at all times remain the sole property of the board and that CoreFour is not granted any license or other proprietary right to the board data.

- Further, CoreFour agrees not to create or maintain any data derivative of the board's data except for the purpose of performing its obligations under its agreement with, and as authorized by, the board, and that any such derivative shall be deemed to be board data.

Collection, use and disclosure

[92] The Confidentiality and Security Agreement between the board and CoreFour binds CoreFour to comply with the *Act* and all board policies and procedures regarding the collection, use and disclosure of personal information under the board's control. The Confidentiality and Security Agreement specifically provides that:

> Under no circumstances shall the Company [CoreFour] or its employees disclose personal information under the control of the board.

[93] The Amending Agreement contains additional provisions requiring CoreFour to ensure compliance with relevant regulations and the security and privacy of the data held by any third party contractors.

[94] The Confidentiality and Security Agreement goes on to state that the *Personal Information* Protection *and Electronic Documents Act* (*PIPEDA*) applies to the collection, use and disclosure of personal information by CoreFour for its own use and/or benefit, but adds that CoreFour will not collect, use or disclose the personal information of students for its own use or benefit.

[95] As noted above, the board submits that neither this latter provision nor any other agreements provide Edsby with any authority or consent to collect, use or disclose information for its own purposes. The board goes on to state that it is not aware of any such collection or use by Edsby that is outside the control of the board. Further, pursuant to the Amending Agreement, if new data sets are derived by Edsby from the personal information of students and/or parents/guardians, the new data remains under the control of the board. In the board's view, this would include any data that might be linked by Edsby to the personal information of students or parents/guardians.

Confidentiality

[96] The Confidentiality and Security Agreement only permits CoreFour's employees or agents employed by CoreFour to be given access to personal information under the control of the board where they require access to perform their duties in relation to the services provided to the board.

[97] This restriction on access has been revised in the Amending Agreement to permit access to personal information by CoreFour's third party contractors, subject to the restrictions set out under the Subcontracting heading below.

Notice of compelled disclosure

[98] There is no provision in any of the contract documents that requires CoreFour to notify the board (or affected individuals for that matter) in the event that it is legally compelled to disclose personal information, in order to permit the board to take preventive action, or that limits the information that must be disclosed. I recommend

that the board rectify this omission so that CoreFour is required to provide the board with prompt notice to allow it to seek a protective order or other appropriate remedy to prevent or limit such disclosure and, further, that CoreFour will disclose only that portion of the confidential information which it is legally compelled to disclose.

Subcontracting

[99] The Amending Agreement provides that CoreFour is "responsible for ensuring compliance with relevant regulations and security and privacy of the data at third parties..." except where the board has directed CoreFour to share data with third parties, in which case the board bears this responsibility.

[100] The Amending Agreement permits CoreFour to engage third parties as subcontractors, but only with the consent of the board for the purposes identified in the agreements between the board and CoreFour and subject to the board's right to evaluate the contractual terms governing third party disclosure, including:

- The definition of what constitutes personal data under applicable privacy protection laws.
- CoreFour's right to audit the third party with respect to data privacy.
- Identifying applicable privacy laws for processing and cross-border transfers of personal data
- Reporting privacy breaches or suspected breaches
- Instructions for security measures for protecting privacy to the same or a higher level of protection required by the board, including technical and organizational measures

Security

[101] The Confidentiality and Security Agreement provides that CoreFour must employ appropriate Security measures as determined by the board to protect the confidentiality of personal information in its possession but under the control of the board. This Agreement also requires CoreFour to indemnify the board in relation to any breach of the agreement.

[102] The Amending Agreement supplements these obligations by:

- Recommending[12] that CoreFour have a security policy based on a generally accepted technical and organizational security standards.

- Requiring CoreFour and its third party contractors to maintain and make available an inventory of all persons who have access to sensitive information and recommending that all such persons have reliability screening commensurate with that required at on-site board locations.

- Requiring CoreFour to provide security breach notification to the board within 48 hours and to cooperate with board's investigation, disclosure to affected parties and remedial measures.

- Making it the responsibility of the board to:

    - Define roles and responsibilities for control and management of access to sensitive data stored off-site or in the cloud.

    - Establish strong password protection for access to the cloud to ensure no shared accounts are used.

    - Conduct periodic and regular reviews of staff access permissions to externally managed sensitive data.

- For significant amounts of data or if a risk assessment indicates significant risk, requiring CoreFour to have security and privacy controls in place and audited by an objective third party.

- Requiring CoreFour's security policy to be submitted to the board for review.

- Requiring CoreFour to have a formal mechanism for identification, authorization, session management and key management aligned with the board.

- Requiring CoreFour and third parties to provide formal documented results from objective assessments of internal/on-site and off- site/cloud-based networks at regular intervals and trigger points for penetration testing and vulnerability scans.

- Stating that CoreFour and third parties storing, processing or transmitting data through the cloud should be compliant with a standardized security policy,

[12] I note that some of the provisions in the Amending Agreement include advisory language taken from the security expert's report. While the board is not obliged to incorporate all of the security expert's recommendations into the contract, in some instances the use of the report's advisory language appears to have introduced potential ambiguity with respect to the parties' rights and obligations. The board may wish to review these provisions with Corefour to remove any ambiguity.

including with respect to the rights of the board to access and delete data, processing data only for the purposes for which it was provided, not using the data for marketing or advertising and the deletion of temporary files.

Retention and destruction

[103] The Confidentiality and Security Agreement provides that CoreFour is required to return or destroy as determined by the board any and all personal information under the control of the board if in CoreFour's possession as a result of services provided to the board.

[104] The Amending Agreement adds a provision requiring a Certificate of Destruction of the board's sensitive data when CoreFour's access to the data is no longer required, and, if return or destruction is prevented by law, a requirement that the information be kept confidential or anonymized and no longer processed.

Audits

[105] The Amending Agreement requires CoreFour to submit to reasonable data security and privacy audits by the board or at the board's request by an independent third party in order to verify compliance with contractual requirements and undertakings and applicable law.

[106] As noted above, the Amending Agreement also requires CoreFour to secure the agreement of third parties that it has the right to audit them with respect to data privacy. Further, all third party products and services handling the board's sensitive data must be subject to an independent security assessment at CoreFour's expense.

Governing law

[107] The Amending Agreement indicates that personal data is subject to applicable privacy laws and that the board may evaluate third party contract provisions with respect to applicable laws for processing data across national borders. I note here that the board's July 2015 RFP provides that the laws of Ontario will govern any dispute regarding non- performance of the agreed requirements, and that the Security and Confidentiality Agreement makes specific reference to the *Act* and to *PIPEDA*, where the latter may apply.

[108] The material I have been provided indicates that CoreFour has undertaken that the information in Edsby will be stored within Canada's geographic and legal and boundaries. However, this has not been made a term of the contract. If the location of data storage was in fact intended to form part of the agreement between the board and CoreFour, this should be set out explicitly in the contract.

[109] Although not addressed in the initial contract documents, the Amending Agreement contains provisions directed at ownership of data, audit requirements,

breach notification, subcontracting and downstream liabilities generally.

[110] The contractual arrangements between the board and CoreFour contain reasonable and appropriate provisions to ensure privacy and security in relation to the personal information of students and their parents or guardians.

[111] While I recommend minor improvements, I am satisfied that the board's contractual arrangements with CoreFour fulfill its duties under the privacy and security provisions of the *Act* and regulations.

Are adequate oversight measures in place?

[112] Statutory and contractual obligations only offer effective privacy and security protection to the extent that they are honoured, monitored and, where deficiencies are identified, enforced and remedied.

[113] As part of my investigation, I asked the board to describe how it ensures that Edsby fulfills its contractual obligations in relation to privacy and security. The board advised as follows:

> YRDSB in collaboration with other Board's (sic) using the Edsby platform have established a user group to ensure that educational privacy and security guidelines are adhered to within the Edsby platform. This User Group has also mandate (sic) that CoreFour/Edsby complete the Independent Security Assessment annually. This is to occur before end of 2019.
>
> *YRDSB Management of Third Parties / Vendors with Access to Sensitive Data* – YRDSB's IT Application and Operations team work in collaboration with our Privacy Office to review and tighten access mechanisms to all sensitive data, on premises or in the cloud.
>
> We have not yet defined our roles/responsible (sic) for control of sensitive data stored offsite or in the cloud. We have a process (not formally documented) that reviews who has the access and identifies who grants the access to the data stored offsite. Our Application Architect establishes enforces the password policy, governs the access to the cloud data and oversees the periodic review of staff that have access and associated permissions.
>
> *Third Party Responsibilities if Accessing Sensitive Data* – this practice will be enforced as part of our annual Vendor Review – facilitated by YRDSB's Procurement team.

[114] This account of the board's oversight measures is short on detail on certain matters. The Amending Agreement sets out numerous obligations agreed to by

CoreFour in relation to the security of the information. It also sets out certain responsibilities that the board has agreed to assume. The board's submissions fall short of convincing me that it has either ensured that CoreFour fulfilled those obligations, or adequately discharged its own responsibilities under the Amending Agreement.

[115] For example, the board states that it has not yet fulfilled its responsibility to define roles and responsibilities for control and management of access to sensitive data stored off-site or in the cloud. Further, it has not confirmed whether CoreFour submitted its security policy to the board for review. Beyond these examples, the board's submissions do not confirm that *any* of the mandatory requirements placed on CoreFour in the Amending Agreement have been fulfilled.

[116] I have particular concerns about the response we received from the board regarding the 2019 Security Audit. During my investigation, the board advised that it contacted CoreFour to get an update on the audit that was to be completed for 2019 and was told that CoreFour had not yet started it. CoreFour explained that it was waiting to see if another client would consent to sharing an extensive security audit on another project. If that did not happen, the board said that it would insist that the audit be completed before the end of the first quarter of 2020. More recently, we have been advised by the board that the global pandemic impacted CoreFour's ability to complete the Security Audit but that it is underway.

[117] In my view, the board should document its oversight measures and, in particular, hold CoreFour to its commitment to conduct an independent security audit and provide it to the board. I will be asking the board to report back to us within three months of receiving this report confirming that it has taken steps to ensure CoreFour's performance of the mandatory requirements in the Amending Agreement, as well as fulfilling its own responsibilities under that Agreement. I will also require confirmation from the board that the independent security audit required under the agreement has been completed to its satisfaction.

[118] Having regard to all of the above, the evidence does not establish that it is adequately monitoring the performance of the contractual security obligations, including by enforcing the review and audit requirements in its agreement with CoreFour. I address these shortcomings in my findings and recommendations below.

Edsby terms of use and privacy policy

[119] As noted earlier in this report, the complainant has expressed concerns that Edsby's privacy policy and terms of use allow it to share information with parent companies, affiliates and third parties and that these documents indicate that student information may be sold or become part of a dataset included in corporate bankruptcy or other corporate transactions. In addition, she is concerned that the privacy policy states that Edsby cannot guarantee or warrant the security of information that is provided or stored on the user's behalf and that any information is transmitted at the user's own risk. The complainant also raises concerns that Edsby reserves the right to

use the data without consent. Underlying many of her concerns is the prospect that students' personal information will be analyzed, misused and monetized, and that the board does not have adequate safeguards in place to protect against this activity.

[120] Some of the concerns the complainant raises relate to a previous privacy policy document that is no longer in effect. The current Edsby privacy policy applicable to the attendance program provides as follows (in part):

- Edsby collects personal information provided by the educational organization, content that users provide and information related to usage of the site.
- Edsby will not sell personal information users provide or disclose it to third parties except as described in its Privacy Policy, as follows:
    - Personal information is accessible to authorized employees of the education organization.
    - Personal information is accessible to authorized employees, consultants or contractors of CoreFour who require it to provide technical support to the education organization or users.
    - Personal information may be provided to other third parties that provide software for extended services supported by Edsby, only where requested and approved by the education organization.
    - Personal information will be provided to legal authorities where required by law.
    - Personal information will be disclosed as necessary to identify, contact or bring legal action against someone who is interfering with CoreFour's rights or property or the rules of the education organization.
    - Personal information may be transferred to a trusted third party to track usage and analyse data to enhance services.
    - Personal information may be transferred in connection with a merger, sale, insolvency or bankruptcy.
    - Non-identifying aggregate information may be used or shared with a third party for business or administrative purposes.
- User accounts are set up using information provided by the education organization
- Edsby does not use or sell information for purposes of advertising

- Only the child's school, designated administrative staff and the child's parents have access to the child's personal information. Students are not allowed to create or modify accounts.

[121] Some of the provisions of this privacy policy (for example, relating to enhancement of services, mergers, acquisitions and bankruptcy) appear to conflict with the terms of the agreement providing that the personal information held by CoreFour is owned by the board. To the extent that there is any conflict between the Edsby Terms of Use and Privacy Policy and CoreFour's contractual obligations to the board, which include compliance with the *Act* and board policies and procedures regarding the collection, use and disclosure of personal information under the board's control, the contract would prevail. In my view, the board's notices and online instructions for parents regarding the use of Edsby would benefit from providing users with a specific assurance to this effect.

[122] I will recommend that the board prominently display in its online notices and instructions for parents regarding the use of Edsby a notice clearly describing the contractual limitations on the handling of personal information under the board's control that prevail over conflicting provisions of Edsby's Terms of Use and Privacy Policy.

Security vulnerability for student photos

[123] The specific security vulnerability discovered and exploited by the complainant, was the result of Edsby application's architecture that permitted the complainant to gain unauthorized access to other students' school profile photos (but apparently not their names or other profile information) through the Edsby portal.

[124] The nature of the vulnerability in question and CoreFour's response and technical fix is summarized in an Edsby "Product Vulnerability Report" which the board provided to us as part of its submissions, as follows (in part):

> *Issue Overview*
>
> On January 15th, 2019 the Edsby team was notified that a parent reported a way to retrieve student profile pictures from Edsby in an unauthenticated browser session.
>
> *Initial Issue Response*
>
> The Edsby engineering team immediately began a review of all software in this area. On that same evening of the day the initial report was received (January 15th) the engineering team identified a path that could be used to provide such access. A preliminary configuration change went live that night that addressed some, but not all paths through which this vulnerability could be exploited. A further change was implemented on Jan. 23rd to strengthen the initial fix.

Vulnerability Confirmation

Through an extensive analysis of Edsby log data, the Edsby team confirmed the parent used the approach that the team found and fixed.

Further log analysis of all logs going back to September 2017 turned up no evidence of any other user ever exploiting this vulnerability.

The Edsby team now has a high level of confidence that this vulnerability is closed on all production systems.

Information at Risk

This vulnerability provided access to a student's profile picture. No meta-data about the student (such as name, Student ID, etc.) was accessible through this path.

Once the proprietary encoded link format to access one student's profile picture was obtained (through browser inspection in an authenticated Edsby session) a person could use the link in an unauthenticated browser session and could attempt to find other profile pictures by trying different but similar ID numbers.

Additional Security Enhancement Steps

This vulnerability relied on the fact that profile picture IDs in Edsby were typically 8 digit numbers assigned in sequential fashion. This enabled the parent's guessing approach to work. Edsby has now changed the way profile picture IDs are assigned. The new profile picture ID format uses .... [redacted] This effectively prevents any further guessing attempts from being successful (both manual and machine generated).

The software to support this new approach is now live on production Edsby servers.

As an added security enhancement .... [redacted]

As a precaution the Edsby development team has done an audit of other parts of Edsby that provide link- based access to resources to ensure each access path has the appropriate permissions and access controls on it. The team will also ensure this is an area of focus as well for our annual independent security penetration testing / audit that will be done in the coming months.

[125] In answer to our question whether this vulnerability has been fully remedied and whether any additional potential vulnerabilities have been identified and remedied, the board refers to Edsby's confirmation in this report that the vulnerability was closed on

all production systems; and states that it is not aware of further potential vulnerabilities of personal information. Based on this assurance, I am satisfied that this vulnerability has been satisfactorily addressed. Further, since there is no evidence the vulnerability resulted in a breach affecting more than the few students the complainant has identified, I see no basis for requiring the board to notify all parents of a temporary and limited security vulnerability.

[126] As noted above, the unauthorized access was possible because student photos were numbered sequentially on the Edsby platform. This allowed the complainant to access other students' profile images by making small changes to the internet address or URL of his own child's profile. The concern was that this security vulnerability could be exploited by bad actors and automated tools to download all student photos in the Edsby database.

[127] I note that a similar vulnerability was identified, and its implications examined, in Investigation Report IR19-01 issued by the Nova Scotia Information and Privacy Commissioner in January 2019[13]. That report examined a series of serious data security breaches on Nova Scotia's new Freedom of Information website. The website allowed users to process access requests for both general and personal information online and to receive access to requested records through links in messages delivered through the website portal. Previously released general records could be accessed by all citizens without the need for an access request, whereas records containing personal information were intended to be released only to the requesting individual to whom they related. A single cloud-based database hosted by a third-party was common to all uploaded documents, both general and personal, except for a unique file identification number assigned to the URL for each document that was uploaded.

[128] The Nova Scotia Commissioner observed that this design was common for websites that enable access to databases storing public information, but contained a significant security vulnerability if used for information intended to be private. A link to a file intended for an individual was delivered in a message through the website portal available only to the individual. Clicking on the link would then take the user to the document and display the full URL in the browser's address bar. However, a user viewing a few document URLs would see that the web address was identical except for the unique document identification number. Further, it was commonly known that small changes to the URLs of these types of websites could give the user access to other documents in the database; and automation tools could make the process of gathering up documents available from this type of database faster.

[129] The Nova Scotia Commissioner concluded that, given the nature of the database and the common knowledge that manipulating document identification numbers may

---

[13] Department of Internal Services (Re), 2019 NSOIPC 2 (CanLII)

allow users to access other data in the database, the risk in that case was foreseeable. She stated that where the decision is made to deploy personal information in electronic format on a website, reasonable security requires "diligent testing and cyber risk assessments to identify and mitigate risks associated with the technology design choices."

[130] In the case before me, it appears that the complainant was able to exploit a similar security vulnerability. Once he gained access to his child's account and the link to his child's photograph as an authenticated user of Edsby, he was able to access the photographs of at least some other students by changing the document number displayed. While there is nothing before me to indicate that the website design for Edsby is the type used in the Nova Scotia case, the design of this component of Edsby is a flaw which, in my view, could have been reasonably anticipated had the board adequately monitored the performance of the contractual security obligations, including by enforcing the review and audit requirements in its agreement with CoreFour.

[131] An additional security vulnerability that warrants mention was referred to by the complainant in his initial complaint. He states that in using the Edsby platform, he was allowed to set a password just by pressing the space bar. While the board established password management policies for teachers and student account users, including password strength requirements, parent accounts are managed by CoreFour/Edsby. Unlike board-issued accounts, parent accounts had weak password requirements which was a security vulnerability because it could facilitate the creation and use of insecure accounts with access to the Edsby platform and data. However, based on the material I have reviewed, I am satisfied that this vulnerability has been resolved.

Summary of findings

1. The information at issue qualifies as "personal information" under section 2(1) of the *Act*.

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

3. The board provided notice of collection as required under section 29(2) of the *Act*.

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

5. The board's disclosure of the information at issue to CoreFour in connection with the Edsby attendance monitoring function is in accordance with section 32 of the *Act*.

6. The board has reasonable contractual measures in place to ensure the privacy and security of the personal information of its students, in accordance with the requirements of section 4(1) of Regulation 460 of the *Act*.

7. The board has not demonstrated that it has reasonable oversight measures in place in relation to the performance of CoreFour's contractual security obligations, including by enforcing the review and audit requirements of its agreement with CoreFour, in accordance with the requirements of the *Act* and its regulations.

Recommendations

1. The board should document the steps that it has taken to ensure CoreFour's fulfillment of the mandatory requirements of the Amending Agreement.

2. The board should document the steps it has taken to fulfill its responsibilities under the Amending Agreement, as discussed in paragraph 115 of this Report.

3. If it has not already done so, the board should require that CoreFour submit to an independent data security and privacy audit and provide its results and conclusions to the board.

4. The board should:

    i. require CoreFour to fully implement all of the security expert's recommendations in its February 2018 assessment, and in particular the security expert's recommendations, as set out at paragraph 86 of this Report; and

    ii. require CoreFour to fully and immediately implement information security policies and controls that are aligned with a generally accepted technical and organizational framework or standard, such as ISO/IEC 27001, and which can be independently audited.

5. The board's agreement with CoreFour should be amended to provide that, in the event that CoreFour is legally compelled to disclose personal information, CoreFour is required to provide the board with prompt notice to allow it to seek a protective order or other appropriate remedy to prevent or limit such disclosure and, further, that CoreFour will disclose only that portion of the confidential information which it is legally compelled to disclose.

6. The board should prominently display in its online notices and instructions for parents regarding the use of Edsby a notice clearly describing the contractual limitations on the handling of personal information under the board's control that prevail over conflicting provisions of Edsby's Terms of Use and Privacy Policy.

7. Within three months of receiving this Report, the board should provide this office with proof of compliance with the above recommendations.

Original Signed by: April 13, 2021

Lucy Costa
Manager of Investigations