Update May 1, 2025

Since our last web update, we've continued to look into the cyber security incident that occurred in December 2024 at Pembina Trails. This includes reviewing the files that were made available on some parts of the internet which we mentioned in our last update and which you may have read about in recent media coverage.

Our preliminary review of these files has identified three broad categories:

Backups of our Student Information System database – about which we informed the community on December 19, 2024 (2014 to 2024 student base) and April 9, 2025 (2011 to 2014 student base).

Excerpts from our staff payroll database – about which we informed staff and the community on December 19, 2024. We still have no evidence that the contents of the database itself were accessed, however, we have identified excerpts in some of the accounting files.

Out of an abundance of caution, we have offered 36 months of credit monitoring service at no cost to current and former staff whose information was in that database.

Student and staff storage files from 12 schools – this is the bulk of the files identified in our initial review. These are files that have been saved in network storage made available to all students and staff at the 12 schools (Vincent Massey, Pembina Trails Collegiate, Acadia, Bairdmore, Crane, Fort Richmond, Oakenwald, Ralph Maybank, St. Avila, South Point, Viscount and Shaftesbury). These miscellaneous files appear to contain mainly educational videos, lesson plans and student assignments accounting for the large volume of digital content.

We've engaged experts to conduct a data mining exercise (i.e., a deep dive using specialized tools and expertise) to search for any further types of information that may require action, such as scans of passports or social insurance numbers. We will contact the individuals concerned directly, if they haven't previously been informed, and provide them with information and tools to help them secure their information.

Since the incident in December, we've been working with a third-party security vendor to enhance some of our existing measures and to provide 24/7 security monitoring of our technology systems. We are pleased to say that our systems remain secure, in keeping with our commitment of minimizing the impact on learning and safeguarding our students' and staff's information.

We would like to acknowledge the support of our community and staff throughout this incident. Unfortunately, organizations across the public and private sectors are being repeatedly targeted by cyber criminals. Nonetheless, we are emerging stronger from this experience, with a cyber resilient mindset which we hope to share with others.

Should you have any questions, please contact our privacy officer using this form.