Holy Name of Mary
College School

Wednesday January 22nd 2025

Dear staff,

This letter is to serve as notification of a data incident at Holy Name of Mary College School (HNMCS) which may impact you. In light of this, we wish to provide you with the following information.

1. **Nature of Data Breach**
   On December 28, 2024, PowerSchool, our Student Information System (SIS) provider, identified a potential cybersecurity incident involving unauthorised access to its customer support portal, caused by a compromised login credential. This vulnerability allowed an unauthorised third party to gain remote access to the school's information system and extrapolate the following information that may directly impact you:

   - Staff data:
     - First Name
     - Last Name
     - Gender
     - Home phone
     - HNMCS email address
     - Address (Street, City, Province and Postcode)

2. **Likely consequences of the breach**
   While PowerSchool believes the accessed data has been deleted without further replication or dissemination, there remains a possibility of misuse of the compromised information. This could include unauthorised use of personal details. However, there is no evidence of continued unauthorised activity in PowerSchool's systems at this time.

3. **Description of measures taken or proposed by the school to address the breach**
   The school is closely monitoring the situation in collaboration with PowerSchool and with assistance from data protection and cybersecurity experts at 9ine. Immediate steps have been taken to address the breach, including:

   Steps taken by PowerSchool

- PowerSchool has engaged its cybersecurity response team and third-party experts.
- Ensuring the compromised credential was deactivated and passwords for the affected portal reset.

- Enhancing password security and access controls for all PowerSource accounts to prevent future occurrences.

Steps taken by HNMCS

- Conducted an incident investigation to understand the scope of the breach and the data affected.
- Notified the Office of the Privacy Commissioner of Canada

We are committed to ensuring our systems and partners' systems remain secure and compliant with data protection standards.

4. **Indication of what measures the school has undertaken to mitigate the possible adverse effects of the breach**

To minimise potential risks, the following mitigations are in place:

- Engaged with the 9ine Cyber and Data Protection Consultants, who continue to monitor the dark web.
- Engaged with PowerSchool to receive credit monitoring services despite the fact that no financial data is stored in the PowerSchool SIS
- Engaged with PowerSchool to receive identity protection services, with more information to follow

5. **How you can protect your data**

We recommend the following good practice steps to protect your information and minimise potential risks:

- **Beware of phishing attempts:** Be cautious of unsolicited emails or calls requesting personal information.
- **Enable multi-factor authentication**: Use two-factor authentication for your online accounts whenever possible.
- **Update passwords**: Change your passwords regularly and use strong, unique passwords for all of your online accounts.
- **Consider using identity protection tools**: Take advantage of the credit monitoring and identity protection services offered by PowerSchool. Details to follow once they are provided by PowerSchool

6. **Data Protection Officer**

For more information regarding this incident you can email Andrew MacLeod, Director of Technology using the email pstech@hnmcs.ca directly

We want to assure you that we conduct thorough due diligence when selecting and monitoring our vendors, ensuring they maintain robust security measures to protect your personal data. For these services we have been working with a company called 9ine, a global specialist in Data Privacy, Cyber Security and Vendor Management, for over 2 years now.

Protecting the privacy and security of your personal information is of utmost importance to us, and we take this matter very seriously.

We will keep you informed of any additional relevant updates that occur involving this incident.

Yours sincerely,
Andrew MacLeod
Director of Technology