PUBLIC NOTICE – COLLÈGE SAINT-CHARLES-GARNIER

Cybersecurity Incident

Collège Saint-Charles-Garnier places great importance on protecting the personal information entrusted to us. In this regard, we wish to inform you of a cybersecurity incident that occurred on March 27, 2025, which may have compromised certain personal information stored in our IT systems. Through this notice, we aim not only to raise awareness within the Collège Saint-Charles-Garnier community about the potential impacts of this incident but also outline the steps you can take to protect your personal information.

What happened and what actions were taken?

On March 27, 2025, our computer systems encountered technical difficulties. In collaboration with third-party cybersecurity experts, we immediately launched an investigation to analyze the incident and identify its causes and scope. The investigation revealed that Collège Saint-Charles-Garnier had fallen victim of a cybersecurity incident, during which an unauthorized third party accessed data stored on our systems.

Unfortunately, the investigation was unable to determine precisely which of the data stored on our systems had been compromised. In this context, we have chosen to act with the utmost caution and transparency by notifying all individuals about whom we hold sensitive information in computer format.

We have therefore carried out a rigorous analysis of all the computer data stored, which has enabled us to identify the individuals concerned and the nature of the personal information concerning them.

What personal information is affected?

As previously mentioned, some of our data may have been compromised, although we are unable to determine exactly what could have been accessed. The data is as follows:

- Full name;
- Residential address;
- Email address;
- Phone number(s).

Moreover, depending on the category to which you belong (student, parent, employee or client of the parking service or language courses), different types of personal information may be involved:

- Current/former students:
    - Date of birth;
    - Social Insurance Number (SIN);
    - Permanent code;
    - Health insurance number;
    - Photograph;
    - In certain cases:
        - Health information; and
        - Passport or birth certificate information.
- Current/former parents:
    - Place of birth;
    - Educational or occupational details;
    - Banking information used for authorized debit of tuition fees;
    - In certain cases:

Click or tap here to enter text.

    - Credit card information used to register your child in our *French Summer Program*; and
    - Passport or other financial document information.

- Current/former employees:

    - Date of birth;
    - Social Insurance Number (SIN);
    - Various documents in the employee file (e.g., employment confirmation letters) and information related to benefits (e.g., pension fund);
    - In certain cases:
        - Banking information used for payroll deposits;
        - Tax information (e.g., T4/R1).

- Clients of the parking service and language courses:
    - Banking information used for authorized debit of parking fees and credit card information used for participation in language courses.

Please note that the list of sensitive information above includes all potential categories of data that may have been affected by this incident. Not all this information applies to every individual. For some individuals, only a portion of this information was impacted, based on the information we had on record for them.

A personalized notice was sent to the individuals affected by the incident, either by email or by mail, based on the contact information available in the records of Collège Saint-Charles-Garnier. This notice outlines the circumstances of the incident, the nature of the potentially affected personal information, the measures taken in response to the incident, and the recommended actions for individuals to protect their personal information. If you believe you may have been affected by the incident but have not received a notice, please contact us at direction@collegegarnier.com.

What can you do?

We encourage you to remain vigilant to common threats to your identity and personal information by taking the following steps:

- Be cautious when sharing your personal information in an unsolicited manner, whether by phone, email or on a website. Never respond to unsolicited requests for your personal information.
- Monitor your bank accounts. If you have any doubts, or if you notice any fraudulent or suspicious transactions on your credit or debit card, we recommend that you contact your financial institution.
- Avoid clicking on links or downloading attachments in suspicious emails.
- If you receive communications that appear to be from Collège Saint-Charles-Garnier, requesting financial or other personal information, and you were not expecting these communications, please consider them fraudulent. Contact us at the coordinates below to confirm authenticity.

The following website offers additional tips and resources to help you protect your identity: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/.

For more information

We regret that this incident has occurred. If you would like more information or believe you may have been affected by the incident but did not receive a notice, please contact us at direction@collegegarnier.com.

Thank you for your understanding.

Sincerely,

The Executive Team

Click or tap here to enter text.