NOTICE OF POWERSCHOOL DATA EVENT IMPACTING
SAINT JOHN VIANNEY HIGH SCHOOL

St John Vianney High School ("SJVHS") recently was informed of an incident that may have impacted the privacy of information related to certain teaching staff and students. While SJVHS is unaware of any actual or attempted misuse of information in relation to the incident, it is providing potentially affected individuals with information about the incident and steps individuals may take to help protect against the possible misuse of this information.

What Happened? On or about January 7, 2025, PowerSchool[1], SJVHS's student information system ("SIS") provider, notified SJVHS that teacher and student information stored in the PowerSchool SIS information tables was accessed and copied to an external location.

While PowerSchool is responsible for this incident and its impact, SJVHS's reaction was immediate upon receipt of the notification, and we continue to investigate and prepare communications as more information is learned. SJVHS understands the importance of your trust and is committed to protecting student and staff data. We are coordinating with PowerSchool, the Diocese of Trenton, and other professional resources to fully address this event.

What Information Was Involved? SJVHS through its own resources is working to determine the nature and extent of the compromised data. This incident may include data related to the Teaching Staff and Students (current and previously enrolled and their parent(s)/guardian) including: name, address, date of birth, phone number, social security number and email. PowerSchool has stated that the incident is contained, they have determined that there is no evidence of malware or continued unauthorized access in the PowerSchool environment, nor do they expect any operational disruption to the services provided to SJVHS.

How Will Individuals Know If They Are Affected By This Incident? PowerSchool advised SJVHS in writing of the incident on January 7, 2025. SJVHS is working to identify all the names of staff and students (current and former), whose data may have been impacted. Those individuals who have been identified as being impacted thus far will receive a notice by US mail and email providing more information.

What You Can Do. SJVHS encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring credit reports for any unauthorized or suspicious activity. Potentially impacted individuals can also review the "*Steps Individuals Can Take to Help Protect Personal Information*" below for further guidance.

PowerSchool will be providing Experian credit monitoring and identity protection services as applicable for educators and students from this organization whose information was involved. Information for enrolling in these services, including an activation code and engagement number, can be accessed at the following link: https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/

For More Information. SJVHS understands individuals may have questions about the incident that are not addressed in this notice. If you have additional questions or need assistance, PowerSchool has set up a toll-free call center, available at (833) 918-9464, from 8:00 a.m. - 8:00 p.m., Central Time, Monday through Friday, excluding major U.S. holidays. Please be prepared to provide the engagement number **B138812.**

[1] PowerSchool is a leading provider of cloud-based software in North America with almost 30 years of expertise providing education technology to more than 18,000 schools and 60+ million students. www.powerschool.com

STEPS INDIVIDUALS CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three (3) major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.