EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Central Catholic High School of Lawrence Inc. ("CCHS") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 19, 2024, CCHS identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on our network between January 14, 2024, and January 19, 2024. Therefore, CCHS engaged in a comprehensive review of the data at risk, with the assistance of its third-party forensic specialists, to assess if any sensitive information could be affected and to whom it relates. As part of this review, CCHS determined on April 10, 2024, that information of certain current and former students, current and former employees and their dependents may be impacted. Since this time, CCHS has taken significant efforts to locate address information for potentially affected individuals to ensure that they are apprised of the incident and steps they can take to protect their information should they feel it is appropriate to do so.

The information that could have been subject to unauthorized access includes name and Social Security number. Please note that we have not received any reports of any misuse of data in connection with this incident.

Notice to Maine Residents

On May 16, 2024, CCHS began providing written notice of this incident to ten (10) individuals. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, CCHS moved quickly to investigate and respond to the incident, assess the security of CCHS systems, and identify potentially affected individuals. Further, CCHS notified federal law enforcement regarding the event. CCHS is also working to implement additional safeguards and training to its employees. CCHS is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CCHS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. CCHS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

CCHS is providing written notice of this incident to relevant state and federal regulators, as necessary.

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF DATA PRIVACY EVENT / NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<last_name>>:

Central Catholic High School of Lawrence Inc. ("CCHS") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? On or about January 19, 2024, CCHS identified suspicious activity in its environment and immediately launched an investigation to determine the nature and scope of the activity. The investigation, which was conducted with the assistance of third-party forensic specialists, determined that an unauthorized actor had the ability to view and acquire certain information stored on our network between January 14, 2024, and January 19, 2024. As a result, and with the assistance of its third-party forensic specialists, CCHS undertook a comprehensive review of data at risk to assess if any sensitive information could be affected and to whom it might relate. As part of this review, CCHS determined on April 10, 2024, that some of your data may be at risk. Since this time, CCHS has taken significant efforts to locate address information for potentially affected individuals to ensure that they are apprised of the incident and steps they can take to help protect their information should they feel it is appropriate to do so.

What Information Was Involved? We determined the type of information potentially impacted by this incident may include the following: <<b2b_text_1 (name, data elements)>>. Please note that we have not received any reports of any misuse of data in connection with this incident.

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Upon discovery of the incident, we immediately commenced an investigation and took steps to implement additional safeguards related to data privacy and security. We also reported this matter to law enforcement and continue to cooperate with their investigation.

In an abundance of caution, we are providing you with access to 12 months of identity monitoring services through Kroll at no cost to you. A description of the services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the activation process yourself as we are not able to activate your services.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* for general guidance. In addition, you can activate the complimentary identity monitoring services being offered through Kroll. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions or need assistance, please contact our call center at: (866) 898-1327, which is available Monday through Friday, between the hours of 9:00 a.m. and 6:30 p.m. Eastern Time, excluding major U.S. holidays. You also may also write to us at 300 Hampshire St, Lawrence, MA 01841.

Sincerely,

Christopher Sullivan
President
Central Catholic High School of Lawrence Inc.

Steps You Can Take to help Protect Personal Information

Activate Identity Monitoring Services

Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three 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 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 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 years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

In incidents where your financial account may be at risk, consumers should take care to monitor their financial accounts closely. You may always contact your financial services provider directly to alert them to monitor for potentially suspicious activity.

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 to five 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, 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 credit freeze, please contact the three 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. This notice has not been delayed by law enforcement.

For District of Columbia Residents: the Attorney General for the District of Columbia may be contacted at Attorney General's Office, 400 6th Street, NW, Washington, DC 20001, (202) 727-3400, https://oag.dc.gov/.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and marylandattorneygeneral.gov

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For *North Carolina* residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC, 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For *Oregon* Residents: the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem 97301-4096, (877) 877- 9392 and www.doj.state.or.us.