Notice of Cybersecurity Incident

October 27, 2025

Dear NSPS Families and Colleagues:

As we continue to recover from a cybersecurity incident that affected our North Stonington Public Schools (NSPS), we thank you for your patience and support during our response to this matter. While the investigation remains ongoing, we are providing this notification to help inform individuals about what happened, what they can expect from NSPS, and how they can protect their personal information going forward.

What Happened:

On or about September 18, 2025, NSPS detected a cybersecurity incident involving unauthorized access to NSPS' network. NSPS quickly engaged cybersecurity responders to assist with securing the network and investigating the incident. The investigation revealed that various NSPS records pertaining to NSPS faculty, staff, and students, were accessed.

Please note, NSPS has no reason to believe that the following resources were affected: Google Classroom, PowerSchool, MySchool Bucks, Arly, Raptor (guest sign in), Family ID, Swiss, Naviance, College Board, Khan Academy, Bridges Math, HMH Reading, IXL, Desmos Math, or Edgenuity.

What Information was Involved:

The investigation revealed that the following types of information may have been exposed:

- Faculty and staff records (current and former), including employment records and personnel files, which may have included name, address, date of birth, payroll and benefits information, tax forms (i.e., Form W-4), and FMLA records. These records may have contained full name, address, Social Security Number, and driver's license information, supplied in relation to NSPS employment.

- Student educational records (current and former), including enrollment information, academic records, assignments and exams, attendance, disciplinary, and expulsion records, academic evaluations, progress reports, IEPs and 504 plans, birth certificates and residency verifications, and student health information, including speech, OT, PT, and counseling notes. These records may have contained full name, date of birth, address, student ID number, health information, and names of parents and guardians.

As of this writing, NSPS has not received any reports of identity theft related to the incident.

What We Are Doing:

NSPS has taken steps to respond to the incident and keep our systems secure. We have reported the incident to state and federal authorities and have alerted the major credit bureaus.

To help you further protect your information, NSPS is providing current and former students, faculty, and staff, access to Single Bureau Credit Monitoring services at no charge. These services provide alerts for twenty-four (24) months from the date of enrollment whenever any changes occur to your credit file. These services will be provided by Epiq, a company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in credit monitoring services at no charge, please call **855-720-3518** between the hours of 9:00 am and 9:00 pm Eastern Time, Monday through Friday, excluding major U.S. holidays, and inform our support center that you are current or former NSPS faculty or staff or a current or former NSPS student, and they will provide you with a unique activation code and enrollment instructions. In order for you to receive the monitoring services described above, you must enroll within 90 days of this notice. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information to confirm your identity. Please retain the activation code for reference when enrolling.

Please also see Steps You Can Take to Help Protect Your Information included below.

For More Information:

If you have questions not addressed in this notice, you may call **855-720-3518** between the hours of 9:00 am and 9:00 pm Eastern Time, Monday through Friday, excluding major U.S. holidays.

NSPS takes protecting the information of its faculty, staff, and students seriously and is committed to recovering from this unfortunate occurrence as appropriately and responsibly as possible.

On behalf of the NSPS leadership team, we appreciate your continued patience and support.

Sincerely,

Troy Hopkins
Superintendent
North Stonington Public Schools

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 agencies 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 violators. 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 at 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 residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com
Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov