SEPTEMBER 1, 2023

NOTICE OF DATA BREACH

Deer Lakes School District ("DLSD") is committed to our students and our faculty – as well as protecting the privacy and security of their personal information. We are making individuals aware of an incident that may affect the privacy of certain personal information. We are also providing notice of the event so that potentially affected individuals may take steps to protect their information, should they feel it appropriate to do so.

***What Happened*?** On or about February 10, 2023, we detected a cybersecurity incident impacting our systems. We launched an investigation into the incident with the assistance of third-party independent cybersecurity experts. We concluded our initial investigation and determined that between January 22, 2023, and February 10, 2023, an unauthorized individual accessed our systems and, as a result, obtained some data, including files potentially containing personal information. At that time, we began a comprehensive review of the impacted data to identify all individuals whose information was involved. The review is ongoing and we are in the process of locating the most recent contact information for those individuals to the extent it is available.

What Information Was Involved? The information involved may include, if it was provided to us, first and last name, driver's license number, financial account and routing number, payment card information, username and password, medical information, health insurance information, and Social Security number. ***However, as of now, DLSD is not aware of any reports of identity fraud or identity theft as a result of this incident.***

What DLSD Is Doing. The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. We are in the process of mailing notification letters to affected individuals. Please be aware that this process takes time and affected individuals will receive direct notice of the incident, on a rolling basis, to the extent a last known address available to DLSD. If you believe you were impacted by this incident, please contact the dedicated toll-free helpline (as stated below).

What You Can Do. DLSD is mailing written notice to students and employees whose information was involved in the incident. The notice contains information about the incident, DLSD's response, as well as information and resources to help individuals protect their information. We are offering complimentary identity monitoring and protection services for individuals whose Social Security number was involved in this incident. We recommend that these individuals enroll in the services provided to increase the likelihood that their information remains protected. **If your Social Security number was impacted you should receive a notification letter via U.S. mail (unless we cannot locate your address). The letter will contain instructions for how to enroll in the complimentary identity monitoring services.**

We encourage potentially affected individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements. We also recommend monitoring your free credit reports to detect errors or identify suspicious activity. Individuals may also review and consider the information and resources outlined in the below "*Other Important Information*."

For More Information. For individuals seeking more information or who have questions, please call the dedicated toll-free helpline 1-888-351-0076. The response line is staffed with professionals familiar with this incident and knowledgeable on what individuals can do to help protect against misuse of their information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. In addition, individuals seeking to contact DLSD directly may write to 19 East Union Road, Cheswick, PA 15024.

SEPTEMBER 1, 2023

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not

authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.