



June 5, 2023

Dear Gower Parent/Guardian,

Gower School District was recently made aware of a data security incident that may have impacted limited personal information of 3rd to 8th grade students enrolled in our school district on or between April 18 and May 4, 2023 as well as limited personal information of staff employed during the period of April 18th through May 4, 2023. This letter contains information about the incident, our response, steps to safeguard your information, and safety measures that have been put in place to assure the security of information in the future. Out of an abundance of caution, we have sent this letter to all Gower parents as we know that any data breach is a cause for concern.

This incident was in the form of a ransomware attack involving a local server used to store limited student and staff directory information (First and Last Name and Gower issued email address). Specifically, an unauthorized and unknown offender gained access to approximately 700 records including 3rd to 8th student names and Gower-issued email address. ***At this time, there is no evidence to suggest that the data accessed has been misused or distributed. It is important to note that student email accounts are not accessible outside of the gower62.com domain.*** This is a critical safety feature that has been in place for several years. The server involved in this attack ***did not store*** any other information about your child. ***No Social Security numbers, no telephone or address information, no financial information, no health data, no current course or schedule information, and no course grades or standardized test scores were involved in this incident.*** Such sensitive student information is highly protected and keeping it safe is a top priority.

This incident is being investigated by the appropriate law enforcement authorities, including the Department of Homeland Security (DHS). According to data security experts that have been involved, including law enforcement, the lack of financial information contained in the data decreases the likelihood that the data will be misused. Falling victim to a ransomware attack is a frightening experience, but there has been some sense of relief in that the attack was limited to basic directory information, some of which is already public, resulting in no ransom being paid.

Although the data that was breached did not include any financial information or your child's Social Security number, we know that you may be concerned about fraudulent activity on your child's behalf. Should you choose to do so, a free credit report for your child can be obtained through annualcreditreport.com, a free resource authorized by the federal government. Additionally, the following credit reporting agencies offer a free service allowing you to receive fraud alerts and to freeze access to your child's credit if you believe doing so is necessary:

- Experian - experian.com/fraud, or 1-888-397-3742, or P.O. Box 2002, Allen, TX 75013
- TransUnion - transunion.com/fraud-victim-resources, or 1-833-395-6938, P.O. Box 2000, Chester, PA 19022
- Equifax - equifax.com, or 1-888-378-4329, or P.O. Box 740241, Atlanta, GA 30374

You may also be interested in visiting the Federal Trade Commission (FTC) website at identitytheft.gov for more information about fraud alerts and security freezes from consumer reporting agencies. The FTC can also be contacted at 1-800-FTC-HELP (1-800-382-4357).



Gower School District 62
7700 Clarendon Hills Rd., Willowbrook, IL 60527
(P) 630-986-5383 (F) 630-323-3074
www.gower62.com



We are deeply committed to the security of student information, and have taken several mitigation measures to reduce the risk of this type of incident occurring in the future, including the migration to enterprise cloud services, enhanced network security, ongoing training to prevent phishing, spearfishing, and other attempts at compromising our networks and/or data, more frequent password changes and updates for staff, and the regular monitoring of our network traffic and overall health and stability. Please know that the protection of your child's personal information is a top priority, and although we are a victim in this case, we sincerely regret any concern or inconvenience that this matter may cause you.

Please visit gower62.com/district/parent-information/student-support-services/student-safety/ for more information, including Student Data Privacy laws and policies that regulate and guide our work in this area.

Should you have additional questions regarding this incident, please contact 630-286-4931 to reach our Data Privacy Officer, Ms. Rebecca Laratta, or email dataprivacyofficer@gower62.com, a dedicated account to help manage such issues and monitored by a number of staff including myself. And of course, I can be contacted directly at vsimon@gower62.com or at 630-286-4932 should you have additional questions.

Respectfully,

A handwritten signature in black ink, appearing to read "VS", followed by a horizontal line.

Victor Simon III
Superintendent of Schools



June 5, 2023

Dear Gower Staff Member,

Gower School District was recently made aware of a data security incident that may have impacted limited personal information of 3rd to 8th grade students enrolled in our school district on or between April 18 and May 4, 2023 as well as limited personal information of staff employed during the period of April 18th through May 4, 2023. This letter contains information about the incident, our response, steps to safeguard your information, and safety measures that have been put in place to assure the security of information in the future. Out of an abundance of caution, we have sent this letter to all Gower parents as we know that any data breach is a cause for concern.

This incident was in the form of a ransomware attack involving a local server used to store limited student and staff directory information (First and Last Name and Gower issued email address). Specifically, an unauthorized and unknown offender gained access to approximately 700 records including 3rd to 8th student names and Gower-issued email address as well as staff names and email addresses. ***At this time, there is no evidence to suggest that the data accessed has been misused or distributed.*** It is important to note that student email accounts are not accessible outside of the gower62.com domain. This is a critical safety feature that has been in place for several years. The server involved in this attack ***did not store*** any other information beyond name and Gower email address. ***No Social Security numbers, no telephone or address information, no financial information, no health data, no current course or schedule information, and no course grades or standardized test scores were involved in this incident.*** Such sensitive information is highly protected and keeping it safe is a top priority.

This incident is being investigated by the appropriate law enforcement authorities, including the Department of Homeland Security (DHS). According to data security experts that have been involved, including law enforcement, the lack of financial information contained in the data decreases the likelihood that the data will be misused. Falling victim to a ransomware attack is a frightening experience, but there has been some sense of relief in that the attack was limited to basic directory information, some of which is already public, resulting in no ransom being paid.

Although the data that was breached did not include any financial information or your Social Security number, we know that you may be concerned about fraudulent activity. Should you choose to do so, a free credit report for your child can be obtained through annualcreditreport.com, a free resource authorized by the federal government. Additionally, the following credit reporting agencies offer a free service allowing you to receive fraud alerts and to freeze access to your credit if you believe doing so is necessary:

- Experian - experian.com/fraud, or 1-888-397-3742, or P.O. Box 2002, Allen, TX 75013
- TransUnion - transunion.com/fraud-victim-resources, or 1-833-395-6938, P.O. Box 2000, Chester, PA 19022
- Equifax - equifax.com, or 1-888-378-4329, or P.O. Box 740241, Atlanta, GA 30374

You may also be interested in visiting the Federal Trade Commission (FTC) website at identitytheft.gov for more information about fraud alerts and security freezes from consumer reporting agencies. The FTC can also be contacted at 1-800-FTC-HELP (1-800-382-4357).



Gower School District 62
7700 Clarendon Hills Rd., Willowbrook, IL 60527
(P) 630-986-5383 (F) 630-323-3074
www.gower62.com



We are deeply committed to the security of student and staff information, and have taken several mitigation measures to reduce the risk of this type of incident occurring in the future, including the migration to enterprise cloud services, enhanced network security, ongoing training to prevent phishing, spearphishing, and other attempts at compromising our networks and/or data, more frequent password changes and updates for staff, and the regular monitoring of our network traffic and overall health and stability. Please know that the protection of your personal information is a top priority, and although we are a victim in this case, we sincerely regret any concern or inconvenience that this matter may cause you.

Please visit gower62.com/district/parent-information/student-support-services/student-safety/ for more information, including Student Data Privacy laws and policies that regulate and guide our work in this area.

Should you have additional questions regarding this incident, please contact 630-286-4931 to reach our Data Privacy Officer, Ms. Rebecca Laratta, or email dataprivacyofficer@gower62.com, a dedicated account to help manage such issues and monitored by a number of staff including myself. And of course, I can be contacted directly at vsimon@gower62.com or at 630-286-4932 should you have additional questions.

Respectfully,

A handwritten signature in black ink, appearing to read "VS", followed by a horizontal line.

Victor Simon III
Superintendent of Schools