Network Security Incident 12.15.22

General FAQs

1. **Can you tell me more about what happened / the type of incident?**

LRSD discovered suspicious network activity on November 11, 2022 and immediately implemented our incident response protocol. We also moved impacted devices offline and hired independent computer forensic experts to help us determine the nature and scope of the activity. We have also taken steps to notify law enforcement and will cooperate with any subsequent investigations into this incident.

2. **Was any student or employee data impacted?**

Our forensic partners have determined that some data was taken from our network as part of this incident. At this time, we do not know exactly what information may be at issue, but we are working as quickly as possible to be able to answer this question.

3. **Are student, parent, or teacher data vulnerable?**

At this time, we are still trying to determine what data may have been impacted. However, if, through our investigation, we learn that any student, parent, staff, or contractor data was compromised, we will work with these individuals to provide appropriate resources to protect their personal information.

4. **Why are you just providing this information?**

Once we discovered the suspicious activity, we implemented our response protocols and engaged key partners. Over the past several days, we have remained focused on our investigation to determine the nature and scope of the incident.

5. **Why can't you provide more details?**

Due to the ongoing investigation and potential sensitive nature of the process, we only have limited information to share at this time. We are guided by standard incident response protocols and are committed to addressing all IT-related outages in a secure

and responsible way. This includes sharing information when it is validated and safe to do so.

6. **When will the investigation be complete so you can provide more details?**

We are working on completing the investigation as quickly as possible, but this type of analysis takes time. Please be assured we remain committed to completing this review and taking all appropriate actions in response to our findings.

7. **What have you done to ensure systems are protected?**

We take the security and privacy of student and employee data very seriously. As soon as we became aware of this event, we took steps to protect our network. We deployed additional security controls and threat detection software to strengthen our defenses and monitor our systems while we investigate the attack. As the analysis progresses, we will continue assessing whether there are additional controls we can put in place to further enhance the security of our network.

8. **Was any data exfiltrated from the system?**

Our forensic partners have determined that some data was taken from our network as part of this incident. At this time, we do not know exactly what information may be at issue, but we are working as quickly as possible to be able to answer this question.

9. **Did you contact the FBI?**

We have filed an IC3 report with the FBI and will cooperate with any investigation into this incident.

10. **How and when will you update us?**

Due to the ongoing investigation, we will be limited on what we can publicly share, but we will provide regular updates on this page as new information becomes available.

Updated 12.15.22