Student Data Privacy: Privacy Practices in Action

Incident Response Communications Plan

Your incident response plan should include a process for communicating pertinent information about the incident to appropriate internal stakeholders, external stakeholders involved in any investigation, and to impacted individuals, parents and other community members in accordance with state laws and district policies. The incident response procedure should make clear who is responsible for communications, including ensuring that public notification is conducted in accordance with regulations, and how that is accomplished. Communications templates, to be customized in the event of an incident, are also recommended.

This resource also supports: Trusted Learning Environment Security Practice 5:
The school system has a process in place to communicate data incidents to appropriate stakeholders, in accordance with state law and school system policies.

Examples of Evidence for the Trusted Learning Environment Application:
Incident response procedure that includes a communications plan, explaining who is responsible for ensuring that notification is conducted in accordance with applicable regulation and district policy, and how that is accomplished.

Here are 10 steps to consider when developing your incident response communications plan:

1. **Make Your Contact List**. Gather phone numbers for your internal team members and external supports. Maintain this list as part of or adjacent to the incident response plan.
2. **Understand your legal obligations**. Review your state breach notification requirements.
3. **Consider the students.** If your state breach notification law doesn't address student personal information, work as needed with your superintendent to develop policy for notifying impacted individuals and their parents in the event of a breach of student personal information.
4. **Decide who will communicate**. Communications about a breach should come from one voice in your district, and ideally, the voice would be that of your superintendent.
5. **Consider employee behavior**. Remind employees to report suspicious activity and then avoid idle chatter about it to keep any communications about the incident controlled and deliberate.
6. **Write the notification now.** Draft template incident response notifications, including placeholders for facts specific to an incident that may arise. Focus on capturing the right tone of voice.
7. **Write press holding statements now.** Draft brief statements for the designated incident response communicator to customize for use in responding to press inquiries.
8. **Consider how the message might be received.** Review your draft notification letter and press holding statements to consider only how the recipient might receive the news. Pay careful attention to facts and tone.
9. **Strike the right balance.** Train on incident response communications. Consider how you will coordinate between work needed to investigate and contain an incident and prompt communications.
10. **Stay calm.** When responding to an incident, keep your team calm and focused. It'll help you ensure that you're getting the right facts to the right people to decide when and how to communicate responsibly to the public.

If you don't have an incident response plan, start by doing your homework. Leverage nationally recognized resources, such as the NIST Computer Security Incident Handling Guide and the NIST Incident Response Recommendations and Considerations for Cybersecurity Risk Management for foundational information and guidance to building an incident response plan and managing system and data security incidents. Identify your internal and external support teams, develop your plan, train (and train again), and adjust your plan as needed based on the training outcomes.

Additional resources from the US Department of Education's Privacy Technical Assistance Center:

- Data Breach Response Checklist
- Data Breach Scenario Trainings