GLET Georgia Leaders of Educational Technology COSN GA | K12 Cyber Forward

CATEGORY GUIDE · RESPOND · AREA 19 OF 22 · NIST CSF 2.0 RS.CO

Incident Response Reporting and Communication

This category asks whether you know who to notify during an incident, in what order, and on what timeline — superintendent, board, insurance carrier, state agencies, law enforcement, staff, and families.

Why it matters

- Cyber insurance policies set conditions for giving notice and often require the carrier's approved breach counsel and forensic firms. Hiring outside help before calling the carrier, or waiting too long to call, can put coverage for those costs at risk.
- Students post about outages long before the district office does. A calm, accurate first message to staff and families, sent from pre-approved templates, tells parents whether school is open, buses are running and meals are served, and keeps board members from learning the news on social media.
- Words carry legal weight during an incident. Calling an event a "breach" before counsel has assessed the facts can create notification obligations and public expectations too early, so a matrix that routes every public statement through the superintendent and legal review protects both the district and its families.

Sequencing is high-stakes: many cyber policies require calling the carrier's breach hotline before engaging outside help, a growing number of states require districts to report incidents to state authorities within days or even hours, and parents will hear about an outage from students on social media long before your letter goes out. A prepared communication plan is the difference between a managed story and a board meeting full of surprises.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	No one has decided what counts as a reportable incident or who tells whom. The carrier, the board and families would hear in whatever order calls happened to be made, and statements would be written under pressure. Moving up: Define what counts as a reportable incident and draft the who-to-call list with owners — moving from 'we would figure out who to tell' to written criteria and a developing notification process is the jump to Repeatable.	• No notification list; the carrier's claims hotline is not written down anywhere staff could find it during an outage • No guidance telling staff what to report or how to report it • No prepared messages for staff, families, the media or the board
2 · Repeatable	A draft call list exists, and the district is deciding which events must be reported and to whom. Conversations have started with the carrier, counsel and the communications office about how they would work together. Moving up: Finish and share the process: coordinate notifications with stakeholders in line with the response plan, and brief leadership plus internal and external partners during incidents so everyone works from the same situational awareness.	• Draft first-24-hours call list with names, after-hours numbers and order • Written definition of what staff must report, such as a clicked phishing link, a lost device or an unexpected account lockout, and how to report it • Notes or an email from the broker or carrier confirming notice requirements and panel vendor rules
3 · Defined	A notification matrix, shared with everyone who has a role in it, lists for each severity level who is notified, by whom and how quickly. During an incident, leadership gets regular status updates, and the carrier, counsel and key vendors work from the same facts. Moving up: Turn the process into a managed communication plan: a named owner for each audience, defined success criteria (for example, an internal goal for how quickly families hear from the district, set with counsel), periodic evaluation of how communications performed, and tracked improvement initiatives.	• Notification matrix by severity level with owners and timeframes, distributed to everyone named in it • Status update log from a real incident or tabletop showing regular briefings to the superintendent and the board • Out-of-band contact list for the response team that works if district email and phones are down

Level	What you would see	Artifacts that show it
4 · Managed	Communication runs from a managed plan with an owner for each audience and pre-approved templates. The district sets measures of success, such as how soon staff and families receive a first message, checks performance after each incident and exercise, and tracks the fixes. Moving up: Join the two-way flow: exchange alerts and recommendations with MS-ISAC, K12 SIX, your state's cyber office, and solution providers, and refine your response communications with best practices and tools like mass-notification systems.	• Incident communication plan with pre-approved templates for staff, families, the media and the board, reviewed this year • After-action notes that compare communication performance against the defined measures • Improvement tracker for communication findings with owners and due dates
5 · Optimized	The district both receives and contributes information through groups such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), K12 SIX, state cybersecurity partners and peer districts, and uses what it learns to refine its response communication. Tools such as the family mass-notification system are tested with incident templates so a first message can go out quickly.	• Records of alerts received from, and indicators shared with, information-sharing organizations • Annual review of incident communication against published guidance, with the resulting changes documented • Test sends of incident templates through the mass-notification system, including text and voice versions

Quick wins

Quick win and how	Cost	Effort	Usual owner
Write a one-page 'first 24 hours' call list with names, numbers, and order List in order the incident commander, superintendent, carrier claims hotline, the breach counsel the carrier assigns, board chair, communications lead, principals and key vendors, with an after-hours number for each. Have the superintendent approve the order and keep printed copies with the phone tree.	Free	Hours	Technology director
Pre-draft fill-in-the-blank holding statements and get superintendent sign-off now Draft a staff email, a family message sized for the mass-notification system, a media holding statement and a board briefing outline that say what is known, what families should do today and when the next update will come, without using the word "breach". Have the superintendent and counsel approve them and keep copies offline.	Free	Days	Communications director
Ask your insurance agent to confirm the hotline number, panel counsel rules, and notice deadlines Email the broker or agent asking for the claims hotline, whether panel breach counsel and forensic firms are required, what the policy says about timely notice, and which costs need the carrier's approval before they are incurred. File the written reply with the incident response plan.	Free	Hours	Business and finance officer
Set up an out-of-band group text or encrypted messaging channel using personal numbers for the response team Create the group on personal cell numbers, not district accounts, for the incident commander, backup, superintendent, communications lead and business officer, and send a test message each semester. Agree in advance how decisions made in the group will be copied into the incident record, since those messages may be public records.	Free	Hours	Technology director
Look up and document your state's incident-reporting obligations and deadlines Ask board counsel to list the state and federal notification and reporting obligations that apply to the district, including breach-notification law, whether any Georgia agency must receive a cyber incident report, and notice terms in vendor contracts and the cyber policy. Record each one in the notification matrix with its trigger, recipient and owner.	Free	Days	Legal counsel

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Calling a forensic firm or a lawyer before calling the carrier. Many policies require approved panel vendors, so make the carrier's claims hotline the first external call and use the counsel and forensic firm it assigns.
- Using the word "breach" in the first message. That is a legal determination counsel makes after scoping; say "incident" or "outage" and tell families what they need today, such as schedules, meals and transportation.
- Planning to communicate through systems that may be down. If email, the phone system or the district website is affected, the team needs a pre-built out-of-band group and the mass-notification system's login and vendor support number on paper.
- Letting well-meaning staff speak for the district. Individual emails and social media posts can spread speculation and conflict with counsel's advice; route every external statement through the superintendent and give principals an approved script for their buildings.
- Overlooking state and federal reporting. Beyond family notification, the district may owe reports to state authorities and can report to the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI); follow your counsel, carrier and any state or federal requirements, and log each report with its date and recipient.

Evidence that proves it

- Notification matrix mapping severity to audiences, owners, and deadlines
- Pre-approved template communications: staff email, family letter, media holding statement, board briefing
- Carrier breach-hotline card and panel requirements documented in the IR plan
- State incident-reporting requirements with citations and deadlines in the plan
- Call and notification log from a past incident or tabletop
- MS-ISAC membership confirmation or K12 SIX participation record

Who usually owns it

Superintendent	Approves and delivers external statements, briefs the board, and authorizes family, staff and media notifications.
Communications director	Maintains pre-approved templates, runs the mass-notification system and website updates, and keeps principals supplied with approved talking points.
Legal counsel	Determines whether an event is a reportable breach, identifies required notifications and their timing, and reviews public statements before release.
Technology director	Supplies accurate technical status for every update, maintains the out-of-band channel, and submits reports to the Cybersecurity and Infrastructure Security Agency (CISA), MS-ISAC or state partners as directed.

Insurance relevance · High

Applications ask whether the district has documented procedures for notifying the carrier, law enforcement, state authorities and affected individuals, and the policy wording itself sets notice conditions and vendor requirements. Late notice, or hiring outside firms without the carrier's approval, can lead the carrier to question or decline those costs.

- Do you have documented procedures for notifying the carrier, law enforcement, state authorities and affected individuals after a cyber incident?
- Who is authorized to report a claim, and can they reach the hotline number if district systems are down?
- Does your plan direct staff to use the carrier's approved breach counsel and forensic firms?
- How would you communicate with staff and families if district email and phones were unavailable?

Tip: Make sure the hotline number, notice requirements and panel vendor rules written in your plan match the current policy wording, and recheck them at every renewal.

Funding and free help

CISA K-12 cybersecurity resources and toolkit Always available	Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- Cybersecurity Incidents (Georgia Technology Authority) https://gta.georgia.gov/contact-us/cybersecurity-incidents
- Report a Cyber Incident (CISA) https://myservices.cisa.gov/irf
- Internet Crime Complaint Center (IC3) (FBI) https://www.ic3.gov/
- Data Breach Response: A Guide for Business (FTC) https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
- Protecting Student Privacy (U.S. Department of Education) https://studentprivacy.ed.gov/
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (CIS) https://www.cisecurity.org/ms-isac