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

CATEGORY GUIDE · RECOVER · AREA 22 OF 22 · NIST CSF 2.0 RC.CO

Incident Recovery Communication

This category asks whether you know who tells staff, families, the board, and the press what is happening while systems are being restored — and through what channel when district email and phones may be…

Why it matters

- During recovery, district email, phones and the student information system (SIS) may be unavailable at the moment families most want answers. Without a planned backup channel and a named spokesperson, students and social media set the story, and principals improvise answers that later have to be walked back.
- Early statements can create legal and insurance problems: calling an event a breach before counsel has reviewed the facts, promising that no student data was taken, or releasing details that interfere with a law enforcement investigation. A plan that routes messages through counsel and, where the policy requires, the carrier avoids those mistakes.
- Regular, honest updates keep staff working and families confident about sending children to school, and a plain-language summary after recovery shows the board and community what changed. The same record of who was told what, and when, supports any notification duties to families and staff under federal and state law and district contracts.

Poor communication during recovery does lasting damage: rumors fill the vacuum, families lose trust, and missed notification deadlines under state student-data-privacy and breach laws create legal exposure. Clear, honest, scheduled updates are how a district keeps its community through its worst week.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	Communication during an outage is improvised. No one has decided who speaks for the district, who approves messages or what triggers recovery updates, and contact lists live only in systems that may be down. Moving up: Start building the process: define who triages communication requests and handles media, write action steps for limiting damage from an event, and make sure your draft covers data-breach handling, recovery updates, and staff awareness of PR and privacy policies.	• No written communication plan or designated spokesperson for cyber incidents • Mass-notification contacts depend on a live sync from the SIS, with no recent export kept outside district systems • Staff have never been told where to refer media and parent questions about a technology incident
2 · Repeatable	A communication process is being built. It names who handles the media and how incoming questions are sorted and answered, includes steps for a data breach and for recovery updates, and staff have been reminded of the district's public relations and privacy policies. Moving up: Document the conditions and responsibilities for invoking the recovery plan, and show communications actually reaching internal and external stakeholders, law enforcement, and leadership — with public relations and reputation restoration managed, not improvised.	• Draft procedure covering media inquiries, a triage path for calls and emails from families and staff, and who approves outgoing messages • Breach section listing the steps to take with legal counsel and the insurance carrier before any statement about student or staff data • Staff meeting or training record reminding employees to refer incident questions to the spokesperson and not to discuss student records publicly
3 · Defined	The plan states when it is invoked and who does what, and dated records show recovery updates reaching staff, families, the board, law enforcement and leadership. Rebuilding community trust after an incident is planned, not left to chance. Moving up: Identify channels in advance, build templates from your playbook and tabletop exercises, balance messaging against investigation needs, and turn exercise evaluations into concrete communication improvement initiatives.	• Approved recovery communication plan with invocation conditions, a named spokesperson and alternate, and approvers including legal counsel • Communication log from an exercise or real event recording the time, audience, channel and approver of each message • Post-incident plain-language summary sent to families, or board minutes showing a recovery briefing and the improvements made

Level	What you would see	Artifacts that show it
4 · Managed	Communication is coordinated with the investigation, so updates are timely without releasing details that responders or law enforcement need protected. Channels for each audience are chosen in advance, templates come from exercises, and each exercise produces specific improvements. Moving up: Make improvement cyclical: a documented feedback and communication strategy, gap analysis after every exercise and incident driving measurable change, transparent communication as standard practice, and a playbook of predefined topics ready to restore order.	• Channel list naming the primary and backup channel for staff, families, the board, media, vendors and the state education agency • Template set for staff, families (translated), a media holding statement, the website and a board update, stored on paper and outside district systems • Tabletop after-action report with communication findings turned into an improvement list with owners and due dates
5 · Optimized	Recovery communication improves every cycle. Feedback from staff, principals and families after each exercise or event is gathered and measured, transparency is the default, and a playbook of predefined topics lets the district issue accurate messages quickly.	• Documented feedback strategy, such as a short survey of principals and a sample of families after each event, with results compared to the previous cycle • Tracked measures such as time from decision to first family message and the number of messages that needed correction • Communication playbook with predefined topics such as school closure, payroll status, possible data exposure, meal service and testing schedule changes, reviewed each year

Quick wins

Quick win and how	Cost	Effort	Usual owner
Draft three fill-in-the-blank templates (staff, families, media) and get counsel and insurer sign-off now, not mid-crisis Write short fill-in-the-blank versions that say what is known, what is affected, what people should do and when the next update will come, and avoid words such as breach or stolen until facts are confirmed. Send them to legal counsel, ask your broker or carrier whether the policy requires their review, and keep the approved versions on paper and in a location that does not depend on district accounts.	Free	Days	Communications director
Print a wallet-card contact list: insurer breach hotline, counsel, CISA/MS-ISAC, state agency, spokesperson Collect the insurer's claims or breach hotline and policy number, legal counsel's after-hours number, the Cybersecurity and Infrastructure Security Agency (CISA) reporting contact, your MS-ISAC contact if you are a member, your state education agency contact, local law enforcement and the FBI field office, and the spokesperson and alternate. Print a card for every cabinet member and principal and recheck the numbers each quarter.	Free	Hours	Emergency management lead
Confirm your mass-notification system works without district email or the SIS, and export contact lists monthly From a device off the district network, sign in to the mass-notification platform with an account that does not depend on district single sign-on and send a test message to the cabinet. Export family and staff contact lists, store the export encrypted and outside district systems because it contains personal information, and set a monthly reminder to repeat it.	Free	Hours	Communications director
Add a 30-minute communication segment to your next tabletop or cabinet meeting Use a CISA Tabletop Exercise Package scenario or a simple ransomware scenario and have the group write the first family message, decide who approves it and pick the channel if email is down, timing how long it takes. Record the gaps and assign each fix an owner before the meeting ends.	Free	Hours	Superintendent
Get one signed paragraph from the superintendent stating who may speak publicly and who approves statements Write a short directive naming the spokesperson and an alternate, stating that all other staff refer media and public questions to them, and listing who approves statements: the superintendent, legal counsel and the carrier where the policy requires. Share it with principals and staff and attach it to the recovery communication plan.	Free	Hours	Superintendent

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

Common pitfalls

- Keeping templates and contact lists only in district systems. If identity, email or file servers are offline during the response, the plan cannot be opened; keep printed copies with the superintendent and communications director and a copy somewhere that does not depend on district accounts.
- Saying too much too soon. An early promise that no student data was affected, or use of the word breach before facts are confirmed, may have to be corrected publicly later; say what is known, what is being done and when the next update comes, and have counsel review anything about data.
- Going silent while restoring. Families and staff read silence as bad news and rumors fill the gap; commit to an update schedule and keep it even when the update is that restoration is still in progress.
- Leaving principals and front-office staff without a script. Parents call their school first, and different answers from different buildings undercut the official message; give principals a short talking-points sheet and a clear referral path for media.
- Reaching only part of the community. A single English-language app message misses families who need another language or do not use the app; prepare translated templates for the main languages in your district and use more than one channel, such as automated calls, text, the website and printed notices sent home.

Evidence that proves it

- Recovery communication plan naming the spokesperson, approvers, and the conditions for invoking it
- Pre-approved message templates for staff, families, media, and the board, stored offline and translated
- Printed out-of-band contact roster: cabinet, insurer breach hotline, counsel, MS-ISAC/CISA, law enforcement, key vendors
- Communication log from a real incident or exercise showing timestamps, audiences, and messages sent
- Tabletop after-action report with communication gaps and assigned improvements
- Board minutes or a family letter showing post-incident recovery updates were actually delivered

Who usually owns it

Superintendent	Serves as or names the spokesperson, approves public statements with legal counsel and the carrier where required, and keeps the board informed throughout recovery.
Communications director	Maintains templates, translations, channel lists and contact exports, sends approved messages and keeps the communication log.
Technology director	Supplies accurate, plain-language technical status for each update and confirms the backup communication channels work without district systems.
Legal counsel	Reviews statements about data exposure, advises on notification duties, and coordinates timing with law enforcement and the carrier's breach counsel.

Insurance relevance · Medium

Applications usually reach this area through questions about notification procedures and exercised incident plans rather than public messaging itself. In a claim, the policy's notice and consent conditions and the carrier's breach counsel and notification vendors shape what the district says and when.

- Do you have documented procedures for notifying the carrier, law enforcement, state authorities and affected individuals after a cyber incident?
- Who is authorized to call the carrier's claims or breach hotline, and can they reach it if district systems are down?
- Will you use the carrier's approved breach counsel, forensic and notification vendors, and do you know how to engage them?
- Has your incident plan, including the communication steps, been exercised in the past year?

Tip: If you answer yes to documented notification procedures, make sure the carrier hotline, policy number and the people allowed to call it are written into both the plan and the printed contact card.

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

- CISA Tabletop Exercise Packages (CISA) https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST) https://csrc.nist.gov/pubs/sp/800/61/r3/final
- 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/
- Report a Cyber Incident (CISA) https://myservices.cisa.gov/irf