// FREE SCHOOL RESOURCE

School Cyber Incident Response Pack

First-hour action, recovery, reporting and incident documentation

// WHAT THIS PACK PROVIDES

- A first-hour checklist that separates immediate containment from later investigation.
- Defined leadership, technical, privacy, communications, student-support and vendor roles.
- Playbooks for ransomware, account compromise, phishing, data exposure and third-party incidents.
- Evidence-preservation, communications, CISA/FBI reporting and recovery guidance.
- Printable contact sheets, an incident log, a state-law addendum and an after-action tracker.

// FOR SUPERINTENDENTS, SCHOOL LEADERS, IT, PRIVACY, LEGAL, COMMUNICATIONS, SAFETY, FINANCE AND VENDOR TEAMS

// START HERE

How to use this pack

A practical adoption template - not legal advice or a replacement for district policy

Cyber incidents belong in emergency planning, not only in the IT department.

The U.S. Department of Education reports that school districts experience an average of five cyber incidents per week and recommends integrating cybersecurity into emergency operations planning. [1][2]

Six operating principles

01 **Protect people and essential services.** Address life safety, student supervision, transportation, meals, medication, payroll and emergency communications.

02 **Assign one incident lead.** Technical staff contain the incident; leadership coordinates district decisions.

03 **Contain without destroying evidence.** Isolate affected systems, preserve logs and avoid unnecessary wiping or cleanup.

04 **Use trusted communications.** Move to an out-of-band channel if district email or identity systems may be compromised.

05 **Communicate verified facts.** State what is known, unknown, being done and when the next update will be provided.

06 **Document every material action.** Record times, decisions, approvals, evidence references and restoration steps.

Adopt it before an incident

- [ ] Name the pack owner and incident lead.
- [ ] Complete the contact sheet and state addendum.
- [ ] Align it with the district EOP and Cyber Annex.
- [ ] Confirm insurance and vendor reporting steps.
- [ ] Approve communications and legal review paths.
- [ ] Exercise the first-hour checklist at least annually.

Important. State breach, education, public-records and ransom-reporting requirements vary. District counsel or the appropriate state authority should verify the state addendum before adoption.

// VERSION CONTROL

District / school: _____

Owner: _____

Approved by: _____

Effective date: _____

Review date: _____

Next exercise: _____

// PREPARE NOW

Readiness before an incident

Complete this page and keep a printed copy with the district emergency plan

The first hour is easier when the district has clean contact information, offline recovery options and clear authority. Federal K-12 guidance recommends developing and exercising a Cyber Annex and incident response plan, including practice restoring critical systems from backups. [2]

Operational readiness

- ☐ Critical systems and data owners are documented.
- ☐ Network, cloud and vendor diagrams are current.
- ☐ Offline or otherwise isolated backups are tested.
- ☐ Identity, email and privileged accounts have MFA.
- ☐ Security logs are retained long enough to investigate.
- ☐ A clean laptop and clean communications account are available.
- ☐ Emergency paper processes exist for attendance, transportation, meals and medication.
- ☐ Cyber insurance notice requirements are documented.
- ☐ Vendor breach-notification clauses and emergency contacts are accessible.
- ☐ Local, state and federal reporting contacts are printed.

Authority and decision rights

- ☐ Who may isolate districtwide network segments?
- ☐ Who may suspend cloud services or disable accounts?
- ☐ Who can declare continuity procedures?
- ☐ Who contacts law enforcement and CISA?
- ☐ Who contacts insurance, counsel and vendors?
- ☐ Who approves staff, family, board and media notices?
- ☐ Who may authorize forensic or recovery vendors?
- ☐ Who makes any ransom-related decision?

Do not leave these decisions to an improvised group chat during the incident.

// QUICK CONTACT SHEET

ROLE / ORGANIZATION	PRIMARY CONTACT	PHONE	OUT-OF-BAND EMAIL	BACKUP
Superintendent / executive				
Incident lead / technology				
Privacy / legal counsel				
Communications lead				
Cyber insurance / broker				
Forensics / recovery vendor				
State education / cyber contact				
Local law enforcement / FBI				

Roles and responsibilities

Small districts may combine roles, but every responsibility still needs an owner

One incident lead. One approved situation record. One spokesperson. Parallel technical, legal and communications work should feed a shared decision process.

ROLE	CORE RESPONSIBILITIES	FIRST-HOUR DECISIONS / OUTPUTS
Executive lead Superintendent or designee	Declares activation level, protects district operations, allocates authority and resources, keeps the board appropriately informed.	Activation level; continuity decisions; executive approvals; next briefing time.
Incident lead Technology or security lead	Coordinates response, maintains operational picture, assigns technical work, manages incident log and briefings.	Scope hypothesis; containment plan; action owners; reporting recommendation.
Technical / forensics	Isolates systems, preserves evidence, analyzes logs, identifies affected accounts and systems, supports clean restoration.	Affected assets; indicators; evidence list; containment status.
Privacy / legal	Assesses FERPA, state breach laws, contracts, law-enforcement coordination, privilege and notification requirements.	Legal hold; required reports; notification timeline; approved data use.
Communications	Prepares staff, family, board, media and website messaging; controls rumor response and update cadence.	Holding statement; audience sequence; spokesperson; next update.
School operations	Maintains student supervision, attendance, transportation, food, facilities, testing and continuity of learning.	Manual workarounds; campus instructions; service priorities.
Student / staff support	Addresses safety, counseling, identity-theft support, accommodations and wellbeing impacts.	High-risk individuals; support route; caregiver coordination.
Finance / insurance	Contacts insurer, preserves financial records, stops fraudulent transactions and tracks incident costs.	Insurance notice; bank actions; purchase authority; cost code.
Vendor / cloud liaison	Obtains provider logs, containment support, contractual notifications and restoration commitments.	Vendor ticket; preservation request; service status; escalation path.

Briefing format

Known: verified facts and affected services.

Unknown: material questions still being tested.

Actions: completed, in progress and blocked.

Decisions: required now, by whom and by when.

Avoid role confusion

Technical staff should not independently publish breach conclusions. Communications staff should not promise restoration times without technical validation. Leaders should not direct destructive cleanup that prevents investigation.

// ACTIVATION

Classify and escalate

Do not wait for complete certainty before beginning containment and documentation

LEVEL	TYPICAL CONDITION	EXAMPLES	MINIMUM ACTIVATION
1	**Suspicious event** No verified compromise or operational impact.	Blocked phishing, isolated malware alert, failed login spike.	IT review, ticket, preserve relevant logs.
2	**Contained incident** Limited compromise with manageable impact.	Single account takeover, one lost managed device, contained malware.	Incident lead, privacy review as needed, incident log.
3	**Major incident** Material data, service or multi-campus risk.	Privileged account compromise, suspected data theft, payroll diversion, major vendor breach.	Executive, legal/privacy, communications, insurance, federal/state reporting review.
4	**Critical emergency** Districtwide disruption, active extortion or safety impact.	Ransomware, identity outage, emergency communications failure, widespread exposure.	Full incident team, continuity plan, CISA/FBI and state coordination.

Immediate escalation triggers

- Life safety, threats, stalking or physical security concerns.
- Ransom note, data-extortion claim or widespread encryption.
- Compromise of administrator, superintendent, finance or identity accounts.
- Student or employee PII may have been accessed or disclosed.
- Payroll, benefits, banking or vendor payment instructions changed.
- Multiple campuses or critical services are unavailable.
- A third party reports a breach affecting district data.
- Media, parents or threat actors are already contacting the district.

Decision path

1. **Physical danger?** Call 911 or local law enforcement immediately.
2. **Active spread?** Isolate affected systems and accounts.
3. **Service disruption?** Activate continuity workarounds.
4. **Possible data exposure?** Involve privacy and legal leads.
5. **Criminal activity or ransomware?** Report to CISA/FBI and applicable state contacts.
6. **Public interest?** Prepare an approved holding statement.

Classification can change. Record the initial level, the evidence supporting it and every later change. Under-classifying an incident can delay reporting and continuity actions.

// FIRST HOUR

The first-hour checklist

Contain, preserve, coordinate and keep essential school services operating

0-10 MINUTES | RECOGNIZE AND ACTIVATE

Notify the incident lead.

Use a trusted channel and state what was observed, when and by whom.

Check immediate safety.

Call 911 for physical danger. Protect student supervision and emergency services.

Open the incident log.

Assign an incident ID, recorder, time zone and secure evidence location.

Move off compromised channels.

Use phone, clean accounts or another approved out-of-band method.

10-30 MINUTES | CONTAIN AND PRESERVE

Identify affected systems and accounts.

Start with identity, email, network management, servers, cloud consoles and backups.

Isolate affected systems.

Disconnect from the network. If disconnection is not possible and spread is continuing, power down the device. [5]

Disable or restrict compromised access.

Revoke sessions and tokens; coordinate password changes from a clean device.

Preserve evidence.

Save logs, alerts, email headers, ransom notes, screenshots and relevant system details.

30-60 MINUTES | COORDINATE AND REPORT

Classify the incident.

Estimate operational, data, safety, financial and public-impact severity.

Activate leadership functions.

Bring in executive, privacy/legal, communications, operations, support and finance roles.

Contact required partners.

Notify insurer and critical vendors; report to CISA/FBI and state contacts as appropriate.

Set the next briefing.

Document knowns, unknowns, actions, decisions, owners and next update time.

Do not: wipe systems, delete messages, reconnect isolated devices, use suspected email, speculate publicly, contact attackers independently, or promise that no data was exposed before scope is verified.

Keep operating: prioritize emergency communications, attendance, transportation, meals, medication, payroll and legally required student services.

Ransomware and data extortion

Assume encryption may be only one part of the incident; data theft and persistence may also be present

Federal guidance: isolate impacted systems immediately, preserve evidence, secure backups and report the incident. The FBI does not support paying ransom because payment does not guarantee data recovery and encourages further criminal activity. [5][7]

Immediate technical actions

- [ ] Disconnect affected devices and segments from wired, wireless and remote access.
- [ ] Protect backup systems, hypervisors, identity services and administrative consoles.
- [ ] Disable compromised accounts, revoke active sessions and restrict privileged access.
- [ ] Preserve ransom notes, extensions, filenames, screenshots, logs and malware samples through approved procedures.
- [ ] Identify the earliest known sign of compromise and likely initial access path.
- [ ] Check for data staging, unusual cloud downloads and outbound transfers.
- [ ] Use clean devices and accounts for response coordination.
- [ ] Do not restore systems until persistence and entry points have been addressed.

Leadership and continuity actions

- [ ] Activate manual school operations and service priorities.
- [ ] Notify cyber insurance before retaining vendors or discussing payment.
- [ ] Contact CISA, the local FBI field office and IC3.
- [ ] Engage privacy/legal review for possible data exfiltration and state notifications.
- [ ] Prepare a short staff and family holding statement using verified facts.
- [ ] Track every cost, outage, decision and external contact.
- [ ] Plan for secondary extortion, leaked data and impersonation attempts.

Ransom decision. Any decision must involve executive leadership, legal counsel, insurance, law enforcement and sanctions/compliance review. Never allow an individual staff member or vendor to negotiate independently.

// CLEAN RECOVERY ORDER

1. **Preserve** — Secure evidence and a reliable timeline before destructive remediation.
2. **Remove access** — Close entry points, persistence, exposed credentials and vulnerable services.
3. **Rebuild** — Use trusted images and verified configurations, not convenience restores.
4. **Rotate secrets** — Prioritize identity, admin, service, backup, API and vendor credentials.
5. **Restore** — Validate clean backups and restore in documented business-priority order.
6. **Monitor** — Increase logging and watch for recurring access, extortion and phishing.

// IDENTITY ATTACKS

Account compromise and payment fraud

Treat identity, email and cloud sessions as evidence, not just passwords to reset

Compromised staff, student or admin account

- [ ] Use a clean device to disable or restrict the account.
- [ ] Revoke active sessions, refresh tokens, app passwords and remembered devices.
- [ ] Reset credentials and verify MFA and recovery methods.
- [ ] Remove malicious inbox rules, forwarding, delegates and OAuth applications.
- [ ] Review sign-ins, cloud audit logs, file access, shared links and privileged changes.
- [ ] Identify messages sent, data accessed and linked systems used by the attacker.
- [ ] Preserve original email headers, logs and suspicious messages.
- [ ] Check other accounts using the same or related credentials.

Business email compromise / payment change

- [ ] Stop pending transfers, payroll changes and vendor payments.
- [ ] Verify instructions using a known telephone number, not the email thread.
- [ ] Notify the bank or payment provider immediately and request recall or hold.
- [ ] Preserve the full message, headers, invoices, bank details and call records.
- [ ] Review mailbox rules and compromised vendor or executive accounts.
- [ ] Report internet-enabled fraud to the FBI through IC3.
- [ ] Notify finance, legal, insurance and affected vendors.

Never approve a payment change only by replying to the message that requested it.

// PRIORITY REVIEW

ACCOUNT TYPE	CHECK IMMEDIATELY	ESCALATE WHEN
Identity / directory admin	New admins, MFA changes, app registrations, conditional-access changes, service principals, federation settings.	Any unauthorized privilege, persistence or cross-tenant access.
Email / executive	Forwarding, delegates, sent/deleted mail, phishing sent internally, sensitive attachments, recovery changes.	External fraud, data access, legal or board communications affected.
Finance / HR / payroll	Bank details, direct deposit, tax forms, vendor master changes, payment approvals and exported records.	Money moved, PII accessed, employee accounts changed.
Student information / learning	Record exports, roster changes, guardian contact changes, shared links, grades, accommodations and discipline data.	PII access, widespread student impact or safety concerns.

Student account compromise. Consider harassment, impersonation, extortion and safety impacts in addition to technical recovery. Involve student-support and safeguarding personnel when appropriate.

// PRIVACY RESPONSE

Data breach and unauthorized disclosure

Contain first, then determine scope, legal obligations and support for affected people

A security incident is not automatically a legally defined breach, but the district should not delay containment while making that determination. U.S. Department of Education resources provide a breach-response checklist for educational agencies and institutions. [10]

1. Stop further access or disclosure.

Disable links, recall messages where possible, isolate systems and suspend affected integrations.

2. Preserve the record.

Retain logs, original messages, files, access lists, vendor notices and the timeline.

3. Identify data and people.

Determine systems, fields, record counts, dates, residents' states and whether minors are affected.

4. Determine what happened.

Was information accessible, viewed, acquired, altered, exfiltrated, published or merely exposed?

5. Activate legal/privacy review.

Assess FERPA, state breach law, student-data statutes, contracts and law-enforcement needs.

6. Coordinate notifications.

Use required timing, recipients, content and delivery methods; avoid unsupported assurances.

7. Support affected people.

Provide a contact route and relevant identity-theft, account-security or counseling support.

8. Document the decision.

Record why notice was or was not required, who approved it and the sources consulted.

Scope questions

- What exact data elements were involved?
- Were records encrypted, and were keys also exposed?
- Can access or acquisition be shown through logs?
- Was data changed, deleted, sold or posted?
- Which states do affected people reside in?
- Did a vendor or subcontractor hold the data?
- Are law enforcement or public-records issues present?

Notification principles

- Use plain language and verified facts.
- Describe what happened and when it was discovered.
- Identify the types of information involved.
- Explain actions taken and practical protective steps.
- Provide a staffed contact route.
- Coordinate required state, attorney-general and education-agency notices.

FERPA and state law are separate analyses. FERPA protects the privacy of education records, while state statutes may impose specific breach definitions, deadlines, regulator reports and resident-notice requirements. [11]

// EVIDENCE

Evidence preservation and chain of custody

Preserve enough to understand, recover, meet legal duties and support law enforcement

NIST recommends collecting and retaining incident evidence according to the organization's preservation procedures and retention policies. Chain of custody records who handled evidence, when, and why it was transferred. [12][13]

Preserve

- [ ] Incident date/time, time zone and discovery source.
- [ ] Affected device names, serials, IPs, users and locations.
- [ ] Identity, email, firewall, VPN, cloud, EDR and application logs.
- [ ] Original suspicious emails with full headers.
- [ ] Ransom note, filenames, extensions and displayed wallet/contact details.
- [ ] Screenshots, alerts and relevant configuration states.
- [ ] Vendor tickets, calls, notices and exported audit data.
- [ ] Copies of public statements and notifications.

Avoid

- [ ] Deleting, editing or forwarding original evidence unnecessarily.
- [ ] Running cleanup tools before required data is captured.
- [ ] Logging into suspect devices with privileged credentials.
- [ ] Using the suspected network to store the only evidence copy.
- [ ] Allowing unrecorded handoffs between staff or vendors.
- [ ] Publishing indicators, student data or vulnerabilities.
- [ ] Attempting deep forensics without trained personnel and authority.

// EVIDENCE REGISTER

EVIDENCE ID	DESCRIPTION / SOURCE	COLLECTED BY	DATE / TIME / ZONE	HASH / SEAL	STORAGE

// TRANSFER / CHAIN OF CUSTODY

EVIDENCE ID	RELEASED BY	RECEIVED BY	DATE / TIME / ZONE	PURPOSE	RETURN / LOCATION

Keep operational copies separate from preserved originals where practical. Record any unavoidable change to a system or file and why it was necessary.

// COMMUNICATIONS

Communications during an incident

Be timely without guessing, minimizing harm or compromising the investigation

Audience and sequence

AUDIENCE	PURPOSE
Incident team	Actions, blockers, risks and decisions.
School leaders / staff	Operational instructions and safe workarounds.
Board / governance	Material impact, oversight and decisions.
Families / students	Service impact, safety, protective steps and support.
Media / public	Verified facts through one spokesperson.
Regulators / law enforcement	Required facts and preserved indicators.

Every update should answer

1. What has been verified?
2. What services or people are affected?
3. What should the audience do now?
4. What is the district doing?
5. What remains unknown?
6. When and where is the next update?

// SAMPLE HOLDING STATEMENTS

Staff operational notice

"The district is investigating a cybersecurity incident affecting _____. Do not use _____ until further notice. Use _____ for approved communications. Do not delete messages or attempt your own technical fixes. The next update will be provided by _____."

Family / public holding statement

"The district identified a cybersecurity incident on _____. We took steps to contain the activity and are working with appropriate specialists and authorities. At this time, _____. We will provide verified updates at _____."

Avoid: naming a suspected attacker, claiming no data was affected before validation, giving precise recovery times without evidence, sharing technical vulnerabilities, or placing student/staff PII in public updates.

Preserve: approved drafts, final notices, timestamps, distribution lists, website versions, media questions and corrections.

// APPROVAL PATH

Drafted by _____ Reviewed by technical lead _____ Privacy/legal _____ Approved by _____

// REPORTING

CISA, FBI and external reporting

Report promptly with the facts available; mark unknown information as unknown

CISA

Report cyber incidents and unusual activity:

cisa.gov/report
1-844-SAY-CISA
(1-844-729-2472)

CISA can support incident coordination and broader threat awareness. [6]

FBI / IC3

Ransomware, phishing, fraud and other cybercrime:

Local FBI field office
ic3.gov
1-800-CALL-FBI for appropriate federal tips

The FBI directs ransomware victims to a local field office and IC3. [7][8]

Emergency

Immediate threat to life or physical safety:

Call 911 and local law enforcement.

Do not delay emergency action while completing cyber reporting forms.

Information to have ready

- District name, location and incident point of contact.
- Discovery time, earliest known activity and time zone.
- Affected systems, campuses, services and users.
- Operational, safety, data and financial impact.
- Known indicators: domains, IPs, hashes, accounts and filenames.
- Ransom note, requested amount and whether payment occurred.
- Evidence of data access, theft, publication or extortion.
- Containment and recovery actions already taken.
- Other agencies, vendors and insurers contacted.

Also check and document

- [ ] State education agency reporting.
- [ ] State CISO, CSIRT, homeland security or cyber command.
- [ ] State attorney general breach portal.
- [ ] State and local law enforcement requirements.
- [ ] Cyber insurance notice and consent requirements.
- [ ] Cloud, SIS, payroll, transportation and other vendor notices.
- [ ] Contractual customer or partner notifications.
- [ ] Public-records retention and legal-hold requirements.

External reporting is not the same as resident notification. CISA/FBI reporting supports response and law enforcement. State law and education rules may separately require regulator, parent, student, employee or resident notices.

// REPORTING RECORD

Agency / organization: _____ Date/time: _____ Confirmation / case number: _____

Contact name: _____ Follow-up due: _____ Owner: _____

// RECOVERY

Recovery and continuity of school operations

Restore deliberately from trusted sources and validate each service before broad reconnection

Recovery is a controlled security decision, not simply turning systems back on. Federal school guidance emphasizes continuity of operations, communications and recovery within the Cyber Annex. [2]

// SERVICE RESTORATION PRIORITY

PRIORITY	SERVICE	CONTINUITY WORKAROUND	RECOVERY OWNER / APPROVAL
1	Life safety and emergency communications	Radios, phones, printed contacts, alternate alerting.	
2	Identity, network control and secure administration	Clean admin accounts, segmented access, approved local procedures.	
3	Attendance, transportation, meals and medication	Paper rosters, manual routing, printed plans and phone trees.	
4	Student information and required services	Approved offline records and controlled minimum access.	
5	Payroll, finance and HR	Bank-verified manual controls and dual approval.	
6	Learning platforms and general productivity	Printed work, alternate approved platforms and staged return.	

Recovery gate

- [ ] Evidence and timeline have been preserved.
- [ ] Initial access and known persistence are addressed.
- [ ] Exposed credentials, secrets and tokens are rotated.
- [ ] Systems are rebuilt or verified clean.
- [ ] Critical vulnerabilities and configurations are corrected.
- [ ] Backups are scanned, validated and tested.
- [ ] Monitoring and alerting are active.
- [ ] Service owner and incident lead approve reconnection.

Phased restoration

1. **Pilot.** Restore a limited clean segment or service.
2. **Validate.** Test security, data integrity and business function.
3. **Expand.** Reconnect by documented priority and dependency.
4. **Monitor.** Watch for recurring indicators, access and data leakage.
5. **Communicate.** Update users on approved access and any required resets.

Do not reconnect a system because it "looks normal." Confirm why it is safe, who approved it, what was tested and how it will be monitored.

// INCIDENT RECORD

Incident log

Use one time zone, record facts separately from assumptions, and never erase an entry

Incident ID: _____ Severity / status: _____

Detected date/time/zone: _____ Detected by: _____

Incident lead: _____ Log recorder: _____

Initial description:

_____

_____

DATE / TIME / ZONE	PERSON	OBSERVATION, ACTION OR DECISION	SYSTEM / ACCOUNT	EVIDENCE ID	APPROVAL / NEXT STEP

Logging rule: corrections should be added as a new dated entry. Record important calls, reports, case numbers, approvals, restoration tests and communications.

// IMPROVE

After-action review and corrective actions

Review promptly while details are fresh, then update the Cyber Annex and response procedures

Review questions

- What happened, and what is the confidence level?
- What systems, people, data and services were affected?
- How and when was the incident detected?
- What allowed initial access or impact?
- What containment actions worked or caused delay?
- Was evidence preserved well enough?
- Were reports and notices timely and accurate?
- Did school continuity procedures protect essential services?
- What vendor, contract, staffing or training gaps appeared?
- What controls would prevent or reduce recurrence?

Required outputs

- [ ] Final incident timeline and impact statement.
- [ ] Root-cause and contributing-factor analysis.
- [ ] List of reports, notifications and case numbers.
- [ ] Recovery validation and remaining risk.
- [ ] Cost, downtime and support impact summary.
- [ ] Corrective-action owners and due dates.
- [ ] Updated contacts, diagrams and vendor procedures.
- [ ] Changes to the EOP Cyber Annex and training plan.
- [ ] Board or governance summary as appropriate.

Federal school guidance recommends conducting an after-action review and report shortly after the incident. [2]

// CORRECTIVE ACTION TRACKER

ID	GAP / LESSON	CORRECTIVE ACTION	OWNER	DUE	STATUS

// REVIEW SIGN-OFF

Review date: _____ Facilitator: _____ Executive owner: _____

Plan updated: _____ Next exercise date: _____ Closure approved: _____

// STATE ADDENDUM

State and local requirements worksheet

Complete from official state sources and have counsel verify before adoption

State requirements are not uniform. A district may need to report to its state education agency, state cyber authority, attorney general, state police or other offices, and may need to notify affected people within state-specific timelines.

REQUIREMENT / CONTACT	OFFICIAL SOURCE, PORTAL OR CONTACT	TRIGGER / DEADLINE / OWNER
State education agency incident reporting		
State CISO / CSIRT / homeland security		
Attorney general breach reporting		
State police / cyber unit / fusion center		
Resident, parent, student or employee notice		
Student-data privacy statute		
Ransomware or ransom-payment reporting		
Public-records, retention and legal-hold rules		

// OFFICIAL STATE EXAMPLES - NOT A 50-STATE SUMMARY

Texas

Texas Education Code Section 11.175 establishes district cybersecurity-policy and coordinator responsibilities and includes reporting/notification provisions for qualifying incidents. Verify the current statute and TEA process. [14][15]

New York

NYSED states that educational agencies should report data incidents defined under Education Law Section 2-d using the Chief Privacy Officer's reporting process. Part 121 includes detailed breach and notification requirements. [16][17]

California

California law requires notice for covered breaches of personal information and requires a sample notice to the Attorney General when more than 500 California residents are notified from a single breach. Verify which code section applies to the district. [18][19]

// DISTRICT JURISDICTIONS

Primary state: _____

Other affected residents' states:

_____

State review owner: _____

// VERIFICATION

Verified by: _____

Title / counsel: _____

Date and source version: _____

// US SOURCES

Federal and state references

Official U.S. government sources used for this pack - verify links and state requirements at adoption

// FEDERAL

[1] U.S. Department of Education, K-12 Cybersecurity.
https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity

[2] U.S. Department of Education REMS TA Center, Cybersecurity for K-12 Schools and School Districts: Developing a Cyber Annex.
https://www.ed.gov/media/document/rems-k-12-schools-and-school-districts-developing-cyber-annex-fact-sheet-508c-2023-113278.pdf

[3] U.S. Department of Education REMS TA Center, Ransomware Attacks and the Importance of Collaboration in District-Level Cybersecurity Risk Management.
https://www.ed.gov/media/document/rems-k-12-ransomware-attacks-and-importance-of-collaboration-district-level-cybersecurity-risk-management-2024-113457.pdf

[4] Cybersecurity and Infrastructure Security Agency, Cybersecurity for K-12 Education.
https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity

[5] CISA, Ransomware Response Checklist.
https://www.cisa.gov/ransomware-response-checklist

[6] CISA, Reporting a Cyber Incident.
https://www.cisa.gov/reporting-cyber-incident

[7] Federal Bureau of Investigation, Ransomware.
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

[8] Federal Bureau of Investigation, Contact Us / field offices and cybercrime reporting.
https://www.fbi.gov/contact-us | https://www.ic3.gov/

[9] U.S. Department of Education, Student Privacy Policy Office, Data Security: K-12 and Higher Education.
https://studentprivacy.ed.gov/data-security-k-12-and-higher-education

[10] U.S. Department of Education, Data Breach Response Checklist.
https://studentprivacy.ed.gov/resources/data-breach-response-checklist

[11] U.S. Department of Education, FERPA and protecting student privacy.
https://studentprivacy.ed.gov/

[12] National Institute of Standards and Technology, SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management.
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r3.pdf

[13] NIST, SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.
https://csrc.nist.gov/pubs/sp/800/86/final

// STATE EXAMPLES

[14] Texas Legislature, Education Code Section 11.175. https://statutes.capitol.texas.gov/GetStatute.aspx?Code=ED&Value=11.175

[15] Texas Education Agency, K-12 Cybersecurity Initiative. https://tea.texas.gov/curriculum-and-instruction/learning-support-and-programs/technology-planning/k-12-cybersecurity-initiative

[16] New York State Education Department, Educational Agencies: Report a Data Incident. https://www.nysed.gov/data-privacy-security/educational-agencies-report-data-incident

[17] New York State Senate, Education Law Section 2-d. https://www.nysenate.gov/legislation/laws/EDN/2-D

[18] California Department of Justice, Data Security Breach Reporting. https://oag.ca.gov/privacy/databreach/reporting

[19] California Legislative Information, Civil Code Section 1798.82. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

Resource status: Free school resource. Districts may adapt this pack for internal use. Review against current federal, state, local, insurance and contractual requirements before formal adoption.