NetPropriate®
DISCOVER HIDDEN DIGITAL RISK | FIND PREDATORY BEHAVIOR

NetPropriate Digital Risk Response Packet

Practical walkthrough guides for districts, JPAs, HR teams, legal counsel, administrators, and risk managers

This packet brings together NetPropriate's core response guides for situations involving inappropriate, high-risk, or potentially unlawful digital content identified on a district-managed device, account, or network. The goal is to help authorized response teams preserve records, protect students, limit access, escalate appropriately, and document their response without improvising under pressure.

How to Use This Packet

Start with the Immediate Response Guide when an alert first comes in. Then use the role-specific guides for HR, legal counsel, administrators, JPAs/risk managers, and evidence preservation as the response is routed through the appropriate internal and external channels.

Packet Contents

- Immediate Response Guide — what to do in the first hour after a digital risk alert.
- HR Team Response Guide — employee access, leave, documentation, and labor coordination.
- Legal Counsel Response Guide — preservation, privilege, evidence control, reporting considerations, and escalation decisions.
- Administrator Response Guide — student safety, communications, board awareness, and internal coordination.
- JPAs & Risk Managers Response Guide — district consistency, claim awareness, and risk reduction.
- Evidence Preservation Response Guide — what not to touch, what to preserve, and how to protect chain of custody.
- Disclaimer and Use of Materials — master disclaimer for packet use.

Immediate Response Guide

What to Do in the First Hour After a Digital Risk Alert

1. Purpose of This Guide

When inappropriate, high-risk, or potentially unlawful digital content is identified on a district-managed device, account, or network, the first hour matters.

The district does not need to solve the entire issue immediately. The district does need to slow the situation down, preserve evidence, protect students and staff, involve the right people, and avoid preventable mistakes.

This guide is intended to help districts, JPAs, HR teams, administrators, legal counsel, IT personnel, and other authorized response personnel understand the immediate response steps after a digital risk alert.

This guide is not legal advice, forensic advice, law enforcement direction, employment advice, insurance advice, or mandated reporting instruction. Districts should follow their own policies, legal counsel's direction, law enforcement or child protective agency direction, applicable reporting obligations, and any JPA, insurer, or risk-pool requirements.

Immediate Response Scope Note

This guide is provided for general first-response planning purposes only. NetPropriate does not provide legal advice, forensic advice, law enforcement direction, employment advice, insurance advice, claims-handling direction, mandated reporting instruction, or investigative direction. NetPropriate does not determine whether content is criminal, whether abuse or misconduct occurred, whether discipline is appropriate, whether evidence is admissible, or whether a specific report, notice, or external escalation must be made. All decisions involving student safety, employee access, administrative leave, mandated reporting, law enforcement contact, forensic handling, legal holds, credentialing reports, board notification, public communication, JPA/insurance notice, claims handling, or employment action should be made by the appropriate district officials in coordination with legal counsel, HR, mandated reporters, law enforcement, child protective agencies, JPAs/risk pools, insurers, qualified forensic professionals, or other authorized entities.

2. The First Response Principle

After a digital risk alert, the safest immediate response is:

Stop. Preserve. Limit access. Escalate. Document.

The district should not rush to prove, disprove, explain, minimize, or internally investigate the alert. The first objective is to protect the integrity of the process.

A digital risk alert may become an HR matter, student-safety matter, legal matter, law enforcement matter, child-protection matter, credentialing matter, insurance/JPA matter, or some combination of those categories.

The district's response should begin with structure, not panic.

3. First 15 Minutes: Stabilize

Within the first 15 minutes after receiving an alert, the district should focus on immediate containment and routing.

A. Confirm receipt of the alert

The person receiving the alert should document:

- Date and time received;
- Who received it;

- User or employee associated with the alert;
- Device, account, or network location involved;
- General alert category;
- Whether the matter appears to involve student safety, suspected child exploitation, threats, or urgent risk;
- Who was notified next.

The recipient should avoid adding speculation, assumptions, or legal conclusions.

B. Do not open or forward suspected content

Personnel should not open, preview, copy, screenshot, email, forward, delete, rename, quarantine, or move suspicious content.

This is especially important if the material may involve suspected child sexual abuse material, child exploitation, or unlawful content involving minors.

C. Notify the designated response lead

The alert should be routed to the district's designated response lead or internal response team.

Depending on the district's structure, the response team may include:

- Superintendent or designee;
- District legal counsel;
- HR director;
- IT director or technology lead;
- Site administrator, where appropriate;
- Risk manager or JPA representative;
- Communications/public information officer, if needed.

The response group should be limited to personnel with a legitimate need to know.

4. First Hour: Preserve and Escalate

Within the first hour, the district should preserve the device, account, alert record, and related logs while escalating the matter through the appropriate channels.

A. Preserve the device or account

If the alert is associated with a district-managed device, the district should identify and secure that device as soon as practicable.

Preservation steps may include:

- Identifying the physical device;
- Recording device make, model, serial number, and asset tag;
- Identifying the assigned user;
- Recording where the device was located;
- Recording whether the device was powered on, asleep, locked, connected, or in use;
- Preventing further normal use;
- Placing the device in a secure location;
- Starting a chain-of-custody record.

Personnel should avoid manipulating the device further unless directed by legal counsel, law enforcement, or qualified forensic personnel.

B. Preserve the alert record

The alert itself should be preserved.

The district should retain:

- Alert date and time;
- Recipient of the alert;
- User/device/account associated with the alert;
- Available file path or metadata;
- Hash-match or category information, if available;
- System-generated details;
- Internal response actions;
- Personnel notified;
- Follow-up assignments.

C. Preserve logs and related records

Relevant logs may age out or be overwritten, so the district should promptly consider preserving:

- Authentication logs;
- Network logs;
- Web-filtering logs;
- Email audit logs;
- Cloud storage records;
- Device login records;
- VPN or remote-access logs;
- Endpoint security logs;
- Student information system access logs, if relevant;
- Administrative action logs.

D. Contact legal counsel

District legal counsel should be involved early when the alert may involve student safety, employee misconduct, suspected child exploitation, possible criminal exposure, credentialing implications, litigation exposure, public communication risk, or insurance/JPA notice.

Counsel can help determine whether the next steps should be administrative, employment-related, forensic, law enforcement-related, child-protection-related, credentialing-related, claims-related, or some combination of those lanes.

5. First 1–4 Hours: Contain Risk

After immediate preservation begins, the district should focus on containment and role clarity.

A. Evaluate student safety

If the user associated with the alert has access to students, the district should evaluate whether immediate student-safety measures are needed.

This may include:

- Removing the employee from student-facing duties;
- Restricting campus access;
- Restricting access to student communication systems;
- Arranging substitute coverage;
- Preserving schedules, rosters, communications, or relevant records;
- Avoiding student interviews until the proper process is determined.

B. Evaluate employee access

HR, legal counsel, and district leadership should determine whether the employee's access should be limited while the matter is reviewed.

Access containment may include:

- District device access;
- Email;
- Cloud storage;
- Student information systems;
- Learning platforms;
- Badge/building access;
- VPN or remote access;
- District-issued phone or messaging tools;
- Administrative systems;
- Shared drives or document repositories.

C. Evaluate administrative leave

If the alert involves an employee, HR and legal counsel should evaluate whether paid administrative leave or another temporary employment action is appropriate.

Administrative leave should be framed neutrally. It is generally a temporary process step, not a final determination of wrongdoing.

D. Limit internal disclosure

Only people with a true response role should receive details.

The district should avoid unnecessary disclosure to staff, board members, parents, community members, or uninvolved administrators before legal counsel and leadership determine what may be shared.

6. Reporting Awareness

Some alerts may trigger external reporting or notification obligations.

Depending on the facts, the district may need to evaluate:

- Mandated child abuse reporting;
- Law enforcement contact;
- Child protective agency contact;
- NCMEC CyberTipline reporting;
- California Commission on Teacher Credentialing reporting;
- Title IX or student-safety procedures;
- JPA, insurer, or risk-pool notice;
- Board notification;
- Parent/guardian notification.

In California, the California Department of Education states that mandated reporters must report known or suspected child abuse or neglect and that the mandated reporter is not responsible for determining whether the allegation is valid before reporting. The CDE also states that reporting only to a supervisor, principal, school counselor, coworker, or other school employee does not satisfy the mandated reporting obligation.

California DOJ materials state that mandated reporters generally must make the initial report by telephone immediately, or as soon as practicably possible, and submit the written report within 36 hours of receiving the information.

For suspected online child exploitation, NCMEC identifies the CyberTipline as the national centralized reporting system for suspected online exploitation of children.

If the employee is certificated, the district should also coordinate with legal counsel and HR regarding whether reporting to the California Commission on Teacher Credentialing may be implicated. CTC guidance states that superintendents must report certain credential-holder changes in employment status due to allegations of misconduct under CCR section 80303.

7. What Not to Do

The district should avoid well-intentioned actions that may compromise evidence, interfere with reporting, or create unnecessary liability.

Personnel should not:

- Open suspicious files to “confirm” what they are;
- Preview images or videos out of curiosity;
- Forward files, screenshots, or descriptions by email;
- Ask IT to search broadly without legal or forensic direction;
- Delete, quarantine, rename, move, or alter suspicious files;
- Wipe, reimage, reset, or redeploy the device;
- Allow the assigned user to continue using the device if containment is warranted;
- Interview the employee before HR and counsel establish the process;
- Question students, witnesses, or staff casually;
- Share details with uninvolved staff;
- Notify parents or the community before communication is reviewed;
- Delay reporting because leadership wants to “confirm more facts” internally;
- Treat the alert as only an IT issue.

The California Department of Education states that school districts and county offices of education do not investigate child abuse allegations or contact the person suspected of abuse or neglect; those responsibilities belong to appropriate investigative agencies.

8. Immediate Role Assignments

The response should have clear lanes.

Legal counsel may coordinate:

- Preservation direction;
- Privilege protocols;
- Reporting analysis;
- Law enforcement or CPS coordination;
- Forensic examiner engagement;
- HR and employment-risk guidance;
- JPA/insurance notice;
- Board, parent, staff, or media communication review.

HR may coordinate:

- Employee classification;
- Administrative leave;
- Employee access restrictions;
- Union or representation issues;
- Personnel documentation;
- Employee communication;
- Credentialing coordination.

IT may coordinate:

- Device identification;
- Account containment;
- Log preservation;
- Alert metadata preservation;
- Asset records;

- Technical documentation;
- Support for forensic preservation.

Administrators may coordinate:

- Student safety;
- Site operations;
- Internal routing;
- Board awareness;
- Communication discipline;
- Parent/community escalation, where authorized.

JPA or risk manager may coordinate:

- Claim notice awareness;
- Risk-pool involvement;
- Approved counsel or vendor requirements;
- Documentation expectations;
- Member-district support;
- Post-incident review.

9. Communication Control

During the initial response, communication should be factual, limited, and coordinated.

Preferred internal language:

> "A digital risk alert was received involving a district-managed device or account. The District is preserving relevant records and coordinating next steps through authorized leadership, HR, IT, and legal counsel."

Avoid language such as:

> "We caught the employee with illegal material."

Unless an authorized legal, administrative, or investigative determination has been made, the district should avoid conclusory, inflammatory, or speculative language.

Suggested holding statement for review

> "The District is aware of a matter involving district technology use and has taken appropriate steps to preserve records, protect students, and involve the appropriate internal and external authorities. Because this matter may involve personnel, student privacy, and/or an active review, the District cannot provide additional details at this time."

Final public-facing language should be reviewed by district counsel and authorized leadership before use.

10. Immediate Documentation Protocol

The district should begin a clean chronological record immediately.

The timeline should document:

- Date and time of alert;
- Who received the alert;
- User, device, account, and location involved;
- Who was notified;
- When legal counsel was contacted;
- When HR was contacted;
- When IT preservation began;
- What device/account actions were taken;

- Whether employee access was restricted;
- Whether student-safety containment was considered;
- Whether mandated reporting was considered or completed;
- Whether law enforcement, CPS, NCMEC, CTC, JPA, insurer, or board notice was considered or completed;
- Who has possession of the device;
- Where the device is stored;
- Next steps assigned.

Documentation should be neutral and factual.

Preferred wording:

> "District personnel received a digital risk alert involving a district-managed device assigned to [employee/user]. The alert was escalated to authorized district leadership, HR, IT, and legal counsel. Preservation and access-control steps were initiated pending further direction."

Avoid speculation about motive, guilt, criminality, or the final meaning of the alert.

11. First 24 Hours: Controlled Follow-Up

Within the first 24 hours, the district should confirm that the immediate response has transitioned into a controlled process.

The district should verify:

- The device and account are preserved;
- Logs and alert records are preserved;
- Chain of custody has begun;
- HR and legal counsel are involved;
- Student safety has been evaluated;
- Employee access has been addressed;
- Reporting obligations have been evaluated;
- JPA/insurance notice has been considered;
- Communications are controlled;
- Board notification has been evaluated;
- A documented timeline exists;
- Any forensic examiner or law enforcement involvement is coordinated;
- No unauthorized personnel are accessing, copying, or discussing suspected content.

The goal is to move from emergency reaction to structured response.

12. Immediate Response Checklist

First 15 Minutes

- Confirm receipt of the alert.
- Document who received it and when.
- Identify the user, device, account, and location involved.
- Do not open, copy, forward, delete, rename, move, or alter suspected content.
- Notify the designated response lead.
- Limit internal disclosure to need-to-know personnel.

First Hour

- Preserve the device, account, alert record, and related metadata.
- Secure the device and prevent further normal use.
- Begin chain-of-custody documentation.
- Notify legal counsel.

- Notify HR if an employee, contractor, volunteer, coach, substitute, or other adult is involved.
- Notify IT for preservation and access-control support.
- Evaluate whether student-safety containment is needed.
- Evaluate whether employee access should be restricted.
- Avoid informal employee, student, or witness interviews.

First 4 Hours

- Confirm relevant logs are preserved.
- Determine whether administrative leave is appropriate.
- Evaluate mandated reporting awareness.
- Evaluate law enforcement, CPS, NCMEC, CTC, JPA, insurer, or board notice.
- Coordinate communications through counsel and authorized leadership.
- Maintain a factual timeline.

First 24 Hours

- Confirm preservation steps are complete or in progress.
- Confirm response roles are assigned.
- Confirm communication limits are in place.
- Confirm external reporting/notice questions have been reviewed.
- Determine whether forensic imaging or outside investigation is needed.
- Document decisions, action items, and next steps.

13. Immediate Response Guiding Principle

The district does not need to have every answer in the first hour.

The district does need to make sure the first hour does not create avoidable harm.

> **Preserve the record. Protect students. Limit access. Involve the right people. Do not improvise. Document every step.**

HR Team Response Guide

Employee Access, Leave, Documentation, and Labor Coordination After an Alert

1. Purpose of This Guide

When inappropriate or high-risk digital content is identified on a district-managed device or account, Human Resources plays a critical role in helping the district respond calmly, consistently, and defensibly.

This guide is intended to help HR teams understand their immediate role after an alert, including employee access coordination, administrative leave considerations, personnel documentation, labor/union coordination, and internal escalation.

This guide is not legal advice and does not replace district policy, collective bargaining obligations, legal counsel, law enforcement direction, mandated reporting obligations, or applicable state and federal requirements.

HR Scope Note

This guide is intended to help Human Resources teams coordinate personnel-related response steps after a digital risk alert, including employee access, administrative leave, documentation, labor coordination, and internal escalation. HR should not independently determine whether content is criminal, whether child abuse or exploitation occurred, or whether an employee is guilty of misconduct. Those determinations should be made through the appropriate legal, administrative, investigative, or law enforcement process.

2. HR's Role After an Alert

HR should not be expected to determine whether the content is criminal, whether abuse occurred, or whether the employee is guilty of misconduct.

HR's role is to help ensure that the district:

- Protects students and staff;
- Preserves the integrity of any employment, administrative, legal, or criminal process;
- Coordinates employee access decisions;
- Maintains appropriate personnel documentation;
- Follows applicable labor and collective bargaining procedures;
- Involves legal counsel and designated leadership promptly;
- Avoids premature conclusions, informal investigations, or unnecessary internal disclosure.

In California, school employees may be mandated reporters, and suspected child abuse or neglect must be reported by the mandated reporter; reporting the concern only to a supervisor or internal administrator does not satisfy the mandated reporting obligation.

3. Immediate HR Priorities

Upon notice of a NetPropriate alert or other report involving inappropriate digital content, HR should coordinate with district leadership and legal counsel to determine the appropriate next steps.

HR's immediate priorities should include:

A. Identify the employee relationship

Determine whether the individual is:

- Certificated;
- Classified;

- Management/confidential;
- Substitute, temporary, volunteer, contractor, vendor, or intern;
- Covered by a collective bargaining agreement;
- Assigned to student-facing duties;
- Responsible for student supervision, transportation, coaching, counseling, technology, or other trusted-access roles.

B. Coordinate access containment

In coordination with legal counsel, IT, and district leadership, HR should determine whether the employee's access should be limited, suspended, or otherwise controlled during review.

This may include access to:

- District devices;
- Email;
- Cloud storage;
- Student information systems;
- Classroom platforms;
- Badge/building access;
- VPN or remote access;
- Administrative systems;
- Shared drives or document repositories;
- District-issued phones or communication platforms.

C. Evaluate administrative leave

HR, in consultation with legal counsel and leadership, should determine whether paid administrative leave or another temporary employment action is appropriate while the matter is reviewed.

Administrative leave should be framed carefully and neutrally. The purpose is generally to protect students, preserve the process, and prevent interference with evidence or witnesses, not to make a final determination of wrongdoing.

D. Preserve employment records

HR should preserve relevant employment records, including:

- Job description;
- Assignment history;
- Site location;
- Supervisor history;
- Prior complaints or discipline;
- Prior investigations;
- Training records;
- Acceptable Use Policy acknowledgments;
- Mandated reporter acknowledgments;
- Technology-use agreements;
- Prior device or access issues;
- Communications about the current alert or concern.

4. What HR Should Not Do

After an alert involving potentially inappropriate or unlawful content, HR should avoid actions that could compromise the investigation, contaminate evidence, or create inconsistent statements.

HR should not:

- Open, view, copy, forward, or distribute suspicious files;

- Ask IT to “dig around” without counsel-directed parameters;
- Interview the employee before counsel and leadership determine the proper process;
- Interview students, witnesses, or staff casually;
- Tell uninvolved staff members about the alert;
- Characterize the employee as guilty;
- Promise confidentiality beyond what law or policy allows;
- Delay escalation because the district wants to “confirm” the content internally;
- Allow the employee continued unsupervised access to students, devices, or records when leadership and counsel determine containment is needed;
- Delete, quarantine, rename, move, or alter files without forensic/legal direction.

The California Department of Education states that school districts and county offices of education do not investigate child abuse allegations or contact the person suspected of abuse or neglect; those responsibilities belong to the appropriate investigative agencies.

5. Mandated Reporting and Escalation Awareness

HR should understand that some alerts may trigger reporting obligations outside the normal employment process.

Depending on the nature of the content or conduct, the district may need to consider:

- Mandated child abuse reporting;
- Law enforcement notification;
- Child protective services notification;
- District legal counsel involvement;
- JPA/risk pool or insurance notice;
- Commission on Teacher Credentialing reporting for certificated employees;
- Internal Title IX, workplace conduct, or student safety procedures;
- Preservation of records for civil, criminal, administrative, or employment proceedings.

For suspected child abuse or neglect in California, mandated reporters are generally required to make an immediate telephone report, or report as soon as practicably possible, and submit the written follow-up report within 36 hours.

HR should not assume that reporting to a supervisor, cabinet member, principal, or HR director satisfies a mandated reporter’s individual reporting obligation.

6. Coordination With Legal Counsel

HR should involve district legal counsel as early as possible when an alert involves suspected inappropriate content, sexual misconduct, student safety concerns, criminal exposure, employee discipline, credentialing consequences, or potential litigation risk.

Counsel may help determine:

- Whether the matter is primarily employment, criminal, student safety, civil liability, credentialing, or all of the above;
- Whether the employee should be placed on paid administrative leave;
- Whether and when the employee should be interviewed;
- Whether a union representative must be notified or present;
- Whether the district should initiate an outside investigation;
- Whether law enforcement or child protective services should be contacted;
- Whether the JPA, insurer, or risk manager should receive notice;
- Whether public records, FERPA, Title IX, or personnel confidentiality issues are implicated;
- How records should be preserved and labeled;
- Who should communicate with the employee.

7. Certificated Employee Considerations

If the employee is certificated, HR should coordinate with the superintendent's office and legal counsel to determine whether reporting to the California Commission on Teacher Credentialing may be required.

The California Commission on Teacher Credentialing identifies superintendent/employing school districts, charter schools, public complaints, self-reported misconduct, and Department of Justice arrest or conviction notices among sources of educator misconduct reports.

California Education Code section 44939.5 also restricts agreements that would prevent mandatory reporting of egregious misconduct or authorize expunging certain egregious misconduct records from personnel files. Recent amendments under AB 2534 address disclosure obligations involving certificated applicants and prior egregious misconduct reporting.

8. Labor and Union Coordination

If the employee is represented by a bargaining unit, HR should review applicable collective bargaining agreements, district policy, and counsel guidance before communicating with the employee or taking employment action.

HR should consider:

- Whether the employee has representation rights during investigatory interviews;
- Whether notice must be provided to the bargaining unit;
- Whether administrative leave language is governed by contract;
- Whether timelines apply to disciplinary action;
- Whether the district must follow a specific progressive discipline or investigation process;
- Whether communications should be issued by HR, the superintendent, site administration, or counsel.

HR should keep the process neutral, factual, and procedurally consistent.

9. Employee Communication Principles

Any communication with the employee should be carefully coordinated with legal counsel and district leadership.

Communications should generally be:

- Brief;
- Neutral;
- Non-accusatory;
- Procedural;
- Consistent with policy and applicable labor agreements;
- Limited to necessary information;
- Clear about temporary access restrictions, leave status, return of district property, and communication expectations.

Suggested neutral framing:

> "The District is reviewing a matter involving district technology use. While that review is pending, the District is placing you on paid administrative leave effective immediately. This action is not a final determination. During this period, you are not to access District systems, contact students, or enter District property unless authorized in writing."

Counsel should review any final language before use.

10. Documentation Protocol

HR should create a clean, chronological record of actions taken.

The HR file should document:

- Date and time HR was notified;
- Who notified HR;
- General nature of the alert;
- Employee name, role, department, location, and supervisor;
- Whether the employee is certificated/classified/represented;
- Immediate access decisions;
- Leave decision and effective time;
- Legal counsel involvement;
- Leadership notifications;
- Union/labor considerations;
- Mandated reporting awareness/escalation;
- Device/account preservation coordination;
- Communications sent to the employee;
- Any reports made to external agencies, as confirmed by counsel or the reporting party;
- Any follow-up actions assigned.

The documentation should avoid speculation, emotional language, or conclusions not yet established.

Preferred language:

> "HR was notified of a digital risk alert involving a district-managed device assigned to [employee]. The matter was escalated to [role/name] and district legal counsel for review. Employee access and leave status were addressed pending further direction."

Avoid language such as:

> "Employee was caught with illegal material."

Unless a final legal or investigative determination has been made, HR records should remain factual and procedural.

11. HR Checklist

Immediate HR Checklist

- Identify employee classification and role.
- Confirm whether the employee has student-facing duties.
- Confirm whether the employee is certificated or classified.
- Determine whether the employee is represented by a bargaining unit.
- Notify district legal counsel and designated leadership.
- Coordinate with IT to suspend or preserve access as directed.
- Determine whether paid administrative leave is appropriate.
- Preserve personnel, policy, training, and technology-use records.
- Limit internal disclosure to need-to-know personnel.
- Avoid employee or witness interviews until the process is set.
- Confirm whether mandated reporting, CTC reporting, law enforcement, CPS, JPA, or insurer notice may be implicated.
- Document every action taken.

12. HR Guiding Principle

HR should treat every serious digital risk alert as both a personnel matter and a potential student-safety, evidence-preservation, and liability matter.

The correct response is not panic.
The correct response is structure.

Preserve the record. Protect students. Limit access. Involve counsel. Follow policy. Document every step.

Legal Counsel Response Guide

Preservation, Privilege, Evidence Control, Reporting Considerations, and Escalation Decisions

1. Purpose of This Guide

When inappropriate, high-risk, or potentially unlawful digital content is identified on a district-managed device, account, or network, legal counsel plays a central role in helping the district preserve evidence, protect student safety, manage employment risk, evaluate reporting obligations, and coordinate with appropriate investigative or governmental authorities.

This guide is intended to help district legal counsel and authorized district leadership think through practical response considerations after a digital risk alert.

This guide is not legal advice from NetPropriate and does not replace the independent judgment of district counsel, special counsel, law enforcement, child protective agencies, forensic examiners, risk-pool representatives, or other authorized entities.

Legal Counsel Scope Note

This guide is provided for general planning and issue-spotting purposes only. NetPropriate does not provide legal advice, act as district counsel, or make determinations regarding criminality, mandated reporting, employee discipline, privilege, evidentiary sufficiency, liability, credentialing consequences, or external reporting obligations. All legal decisions should be made by the district's own legal counsel based on the specific facts, applicable law, district policy, collective bargaining agreements, insurance/JPA requirements, and any direction from authorized agencies.

2. Legal Counsel's Role After an Alert

Legal counsel should help determine whether the district's response should proceed as an employment matter, student-safety matter, criminal referral, child-protection matter, credentialing matter, civil-liability matter, insurance/risk-pool matter, or some combination of those categories.

Counsel's early involvement can help the district:

- Preserve potentially relevant evidence;
- Protect privileged communications where applicable;
- Limit unnecessary internal disclosure;
- Avoid premature factual or legal conclusions;
- Coordinate HR, IT, administrative, and investigative roles;
- Evaluate mandated reporting and external notification obligations;
- Determine whether law enforcement or child protective agencies should be involved;
- Determine whether a forensic examiner should be retained;
- Manage communications with the employee, bargaining unit, board, JPA, insurer, families, media, or community.

3. Immediate Legal Priorities

Upon notice of a digital risk alert, counsel should consider directing the district to preserve the status quo and limit unnecessary access to the underlying material.

Immediate legal priorities may include:

A. Preserve the device, account, alert, and logs

Counsel should work with district leadership and IT to preserve relevant records, including:

- The assigned device;
- User account information;
- File path or hash-match information;
- NetPropriate alert metadata;
- Device serial number and asset tag;
- Assignment history;
- Login history;
- Network logs;
- Web-filtering logs, if applicable;
- Email and cloud-storage records;
- Acceptable Use Policy acknowledgments;
- Prior technology or personnel complaints;
- Chain-of-custody records.

B. Limit unnecessary viewing or handling

Counsel should consider instructing personnel not to open, copy, forward, screenshot, email, delete, rename, move, or further inspect suspicious content unless directed by counsel, law enforcement, or a qualified forensic examiner.

This is especially important where content may involve suspected child sexual abuse material, exploitation, or other unlawful material.

C. Identify the response team

Counsel should identify the smallest appropriate response group, which may include:

- Superintendent or designee;
- HR director;
- IT director or technology lead;
- Site administrator, where appropriate;
- Risk manager or JPA representative;
- Outside counsel;
- Forensic examiner;
- Law enforcement or child protective agency contact, when appropriate.

Internal disclosure should be need-to-know, documented, and role-specific.

4. Response Triage

Counsel should help classify the matter so the district does not treat all alerts the same way.

Potential categories may include:

Category 1: Policy/AUP violation

Examples may include adult pornography, inappropriate personal content, or other prohibited use of a district-managed device that does not appear to involve minors, threats, exploitation, or criminal conduct.

Primary concerns may include:

- Employment discipline;
- AUP enforcement;
- Device misuse;
- Public-record or personnel-record implications;
- Prior notice/training;

- Consistency of enforcement.

Category 2: Student safety or boundary concern

Examples may include content, searches, communications, or digital artifacts suggesting inappropriate interest in students, grooming indicators, boundary violations, harassment, or concerning conduct.

Primary concerns may include:

- Student safety;
- Mandated reporting analysis;
- HR containment;
- Investigation protocol;
- Witness protection;
- Board or leadership notification;
- FERPA/privacy management.

Category 3: Suspected CSAM or child exploitation

Examples may include suspected child sexual abuse material, online enticement, child exploitation, child sex trafficking, or unlawful sexual content involving minors.

Primary concerns may include:

- Immediate preservation;
- Mandated reporting;
- Law enforcement involvement;
- Child protective agency involvement;
- NCMEC CyberTipline considerations;
- Avoiding possession, transmission, or further internal viewing;
- Forensic handling;
- Student-safety containment.

NCMEC describes the CyberTipline as the national centralized reporting system for suspected online child exploitation, including child sexual abuse material, online enticement of children, child sex trafficking, and related categories.

Category 4: Threat, violence, coercion, or extortion concern

Examples may include threats of violence, sextortion, stalking, coercive communications, self-harm indicators, or targeted harassment.

Primary concerns may include:

- Immediate safety assessment;
- Law enforcement contact;
- Threat assessment team involvement;
- Student and staff protection;
- Evidence preservation;
- Communications control.

5. Privilege and Documentation Protocol

Counsel should consider whether and how to structure communications to preserve attorney-client privilege and work-product protection where applicable.

Counsel may wish to direct:

- Who should gather facts;
- Who should receive privileged communications;

- How internal emails should be labeled;
- Whether outside counsel should retain a forensic examiner;
- Whether written summaries should be limited, factual, and non-speculative;
- Whether HR documentation should remain separate from privileged legal analysis;
- Whether board communications should occur in closed session where permitted.

District personnel should avoid broad email chains, speculative comments, emotional descriptions, or premature conclusions.

Preferred internal framing:

> "The District is preserving records and reviewing a digital risk alert involving a district-managed device. Further review is being coordinated through District leadership and counsel."

Avoid:

> "We caught the employee with illegal material."

Unless a final authorized determination has been made, the district should maintain neutral, procedural language.

6. Evidence Control and Forensic Preservation

Counsel should help determine who controls evidence and what should happen to the device or account.

Counsel should consider issuing preservation instructions covering:

- Physical custody of the device;
- Whether the device should be powered off, isolated, or left as-is;
- Whether network access should be disabled;
- Whether passwords, keys, or tokens must be preserved;
- Whether cloud sessions should be terminated;
- Whether email/cloud data should be placed on legal hold;
- Whether backup snapshots or logs should be retained;
- Whether an image should be created by a qualified forensic examiner;
- Who may access the device or data going forward.

The district should document every transfer of custody, including:

- Date and time;
- Person releasing the device;
- Person receiving the device;
- Device description;
- Serial number or asset tag;
- Condition of the device;
- Storage location;
- Reason for transfer.

7. Reporting Considerations

Counsel should help the district identify which reporting and notification duties may apply, while recognizing that some duties may belong to individual mandated reporters rather than the district as an entity.

Potential reporting paths may include:

- Mandated child abuse reporting;
- Law enforcement notification;
- Child protective services notification;
- NCMEC CyberTipline reporting;
- California Commission on Teacher Credentialing reporting;

- Title IX or other internal student-safety processes;
- JPA, insurer, or risk-pool notice;
- Board notification;
- Parent/guardian notification, where appropriate and legally permissible.

In California, mandated reporters must generally report suspected child abuse or neglect immediately, or as soon as practicably possible, by telephone and then prepare and send the written report within 36 hours.

The California Department of Education also states that a mandated reporter's obligation is not satisfied by reporting the concern only to a supervisor, principal, school counselor, coworker, or other school employee.

8. Law Enforcement and Child Protective Agency Coordination

Counsel should help determine whether and when law enforcement or child protective agencies should be contacted.

Where the content may involve CSAM, exploitation, abuse, threats, or imminent safety concerns, counsel should consider whether district personnel should stop internal review and await agency direction.

Counsel should consider addressing:

- Who will make the contact;
- Whether a mandated reporter must separately make the report;
- What information may be shared;
- Whether the district should preserve the device for law enforcement;
- Whether law enforcement wants the device left untouched;
- Whether the district should avoid interviewing the employee or witnesses;
- Whether student interviews should be conducted only by appropriate authorities;
- Whether parent/guardian notification should be delayed or coordinated to avoid compromising an investigation.

The California Department of Education states that school districts and county offices of education do not investigate child abuse allegations or attempt to contact the person suspected of abuse or neglect; those responsibilities belong to appropriate investigative agencies.

9. HR and Employment Coordination

Counsel should coordinate with HR before the district takes employment action or communicates with the employee.

Counsel may need to advise on:

- Paid administrative leave;
- Employee access restrictions;
- Return of district property;
- Communication restrictions;
- Site access restrictions;
- Student-contact restrictions;
- Union or representation rights;
- Notice requirements;
- Investigatory interview timing;
- Progressive discipline or dismissal procedures;
- Separation agreements;
- Credentialing implications;
- Personnel-file preservation.

If the employee is certificated, counsel should consider whether CTC reporting is implicated. The California Commission on Teacher Credentialing states that superintendents/employing school districts are among the sources

of educator misconduct reports, and California regulations require superintendents to report certain changes in employment status for credential holders involving allegations of misconduct.

10. Student Privacy and FERPA Considerations

If the alert or investigation involves student information, counsel should evaluate FERPA and state student-privacy obligations before student records or personally identifiable information are disclosed.

Counsel should consider:

- Whether the information is part of an education record;
- Whether internal recipients have a legitimate educational interest;
- Whether the health or safety emergency exception may apply;
- Whether law enforcement or child protective agencies may receive information;
- Whether the disclosure must be documented;
- Whether parent/guardian communication is required, delayed, limited, or prohibited due to investigative concerns.

The U.S. Department of Education explains that FERPA's health or safety emergency exception permits disclosure of personally identifiable information from education records to appropriate parties when necessary to protect the health or safety of a student or others, but the exception is limited to the period of the emergency and does not authorize blanket release of information.

When a school discloses information under FERPA's health or safety emergency exception, the Department of Education states the school must record the articulable and significant threat that formed the basis for disclosure and the parties to whom the information was disclosed.

11. JPA, Insurance, and Risk-Pool Notice

Counsel should determine whether the district must notify its JPA, insurer, risk pool, or excess carrier.

Potential reasons for notice may include:

- Potential civil claim;
- Employee misconduct allegation;
- Student safety incident;
- Law enforcement referral;
- Credentialing report;
- Media or public-records exposure;
- Board-level concern;
- Potential employment litigation;
- Potential third-party forensic expense;
- Need for panel counsel or approved investigator.

Counsel should review applicable coverage documents, memoranda of coverage, claims-reporting deadlines, reservation-of-rights concerns, and any requirement to use approved counsel, investigators, or forensic vendors.

12. Board and Leadership Communications

Counsel should help determine whether, when, and how the board should be notified.

Counsel should consider:

- Whether the matter is appropriate for closed session;
- Whether the matter involves personnel, litigation exposure, student safety, or law enforcement sensitivity;
- Whether written board materials should be limited or privileged;
- Whether board members should be instructed not to conduct independent inquiries;
- Whether the board should receive a factual status update rather than investigative details;

- Whether public comments, media inquiries, or parent concerns are likely.

Board communications should be careful, factual, and coordinated through counsel and authorized district leadership.

13. Public Records, Media, and Parent Communication

Counsel should help manage external communications.

Counsel may need to coordinate:

- Public Records Act response strategy;
- Personnel-record confidentiality;
- Student-record confidentiality;
- Law enforcement hold or investigative sensitivity;
- Parent/guardian communication;
- Community notification;
- Media holding statements;
- Website or board-meeting messaging;
- Social media monitoring or response.

Suggested holding language for review:

> "The District is aware of a matter involving district technology use and has taken appropriate steps to preserve records, protect students, and involve the appropriate internal and external authorities. Because this matter may involve personnel, student privacy, and/or an active review, the District cannot provide additional details at this time."

Final wording should be reviewed by counsel and district leadership before use.

14. Settlement, Separation, and Personnel-File Considerations

Counsel should exercise caution with settlement agreements, resignation agreements, neutral references, personnel-file language, and any agreement involving confidentiality, non-disparagement, reporting, or expungement.

In California, Education Code section 44939.5 and AB 2534-related amendments address restrictions and disclosure obligations involving egregious misconduct records for certificated employees. Counsel should review current statutory requirements before entering into any agreement involving misconduct, reporting, references, personnel-file contents, or separation terms.

Counsel should also consider whether the matter affects:

- Future employment references;
- CTC reporting;
- Personnel-file retention;
- Substantiated investigation records;
- Credible complaint records;
- Discipline records;
- Settlement confidentiality provisions;
- District responses to future employer inquiries.

15. What Legal Counsel Should Prevent

Counsel should actively help the district avoid common response mistakes.

The district should not:

- Conduct informal internal "confirmation" by opening suspicious files;
- Forward suspected content to HR, administrators, board members, or law enforcement by email;

- Ask IT to search broadly without defined legal/forensic parameters;
- Allow the employee continued access to devices or students if containment is warranted;
- Interview students or the suspected employee before reporting obligations and investigative jurisdiction are evaluated;
- Over-disclose information internally;
- Delay mandated reporting because the district wants more certainty;
- Promise confidentiality to witnesses, families, or employees beyond what law permits;
- Enter into separation terms that interfere with required reporting or record retention;
- Treat the alert as merely an IT support ticket.

16. Legal Counsel Checklist

Immediate Counsel Checklist

- Confirm who received the alert and when.
- Identify the device, user, account, location, and alert type.
- Direct preservation of the device, alert metadata, account data, and logs.
- Restrict unnecessary viewing, copying, forwarding, deletion, or alteration of content.
- Identify the smallest appropriate response team.
- Determine whether immediate student-safety containment is needed.
- Coordinate with HR regarding leave, access, communication, and union issues.
- Evaluate mandated reporting implications.
- Evaluate law enforcement, CPS, NCMEC, CTC, JPA, insurer, or board notice.
- Determine whether a forensic examiner should be retained.
- Protect privileged communications where applicable.
- Preserve personnel, policy, training, and AUP records.
- Create a documented timeline of decisions and actions.
- Manage external communications and public-records risk.
- Review any separation, resignation, or settlement language for compliance.

17. Legal Counsel Guiding Principle

The first legal objective is not to prove the alert.
The first legal objective is to preserve the evidence, protect students, contain risk, and route the matter through the correct legal, administrative, and investigative channels.

> **Preserve first. Limit access. Escalate carefully. Document precisely. Let the right authority make the right determination.**

Administrator Response Guide

Student Safety, Communications, Board Awareness, and Internal Coordination

1. Purpose of This Guide

When inappropriate, high-risk, or potentially unlawful digital content is identified on a district-managed device, account, or network, district administrators may be required to make fast decisions under significant pressure.

This guide is intended to help superintendents, assistant superintendents, cabinet members, principals, site administrators, and other authorized district leaders understand their role after a digital risk alert.

The administrator's role is not to personally investigate the content, determine criminality, or reach premature conclusions. The administrator's role is to help stabilize the situation, protect students and staff, preserve evidence, involve the correct response personnel, and ensure the district follows appropriate legal, HR, reporting, and policy channels.

This guide is not legal advice and does not replace district policy, legal counsel, law enforcement direction, child protective agency direction, mandated reporting obligations, collective bargaining agreements, insurance/JPA requirements, or applicable state and federal law.

Administrator Scope Note

This guide is provided for general coordination and planning purposes only. NetPropriate does not direct administrative action, determine whether abuse or misconduct occurred, decide whether an employee should be disciplined, or determine whether a specific report, notification, or employment action is required. All decisions involving student safety, employee access, mandated reporting, law enforcement contact, board notification, parent communication, media response, or discipline should be made by the appropriate district officials in coordination with legal counsel, HR, law enforcement, child protective agencies, JPAs/risk pools, insurers, and other authorized response entities.

2. Administrator's Role After an Alert

Administrators are often the first leaders expected to "do something." In this context, the most important first action is not to solve the alert immediately. It is to ensure the district does not mishandle the response.

Administrators should help the district:

- Protect students and staff;
- Preserve the device, account, alert, and related records;
- Limit unnecessary access to suspicious content;
- Escalate the matter to legal counsel, HR, IT, and designated leadership;
- Avoid informal investigation or speculation;
- Maintain confidentiality and need-to-know communication;
- Coordinate with the JPA, insurer, or risk pool when appropriate;
- Support mandated reporters without delaying or interfering with reporting obligations;
- Prepare for board, parent, staff, or media communication only when authorized and appropriate.

For California districts, the California Department of Education states that mandated reporters include all school/district employees, administrators, and athletic coaches, and that mandated reporters are required to report known or suspected child abuse or neglect; the CDE also states that the obligation is not satisfied by reporting only to a supervisor or the school.

3. Immediate Administrative Priorities

Upon notice of a NetPropriate alert or similar digital risk concern, administrators should move quickly but carefully.

A. Stabilize the situation

Administrators should confirm that the alert has been routed to the appropriate internal response lead. Depending on district structure, this may include:

- Superintendent or designee;
- HR director;
- District legal counsel;
- IT director or technology lead;
- Site administrator;
- Risk manager or JPA representative;
- Safety/threat assessment team;
- Communications/public information officer.

The response group should be limited to individuals with a legitimate need to know.

B. Protect students and staff

If the employee or user associated with the alert has access to students, staff, sensitive records, facilities, or communication systems, administrators should coordinate with HR and legal counsel to determine whether immediate containment is appropriate.

This may include:

- Removing the employee from student-facing duties;
- Restricting access to campus or certain facilities;
- Suspending access to district systems;
- Preserving district-issued devices;
- Redirecting supervision responsibilities;
- Ensuring students are not placed in a potentially unsafe situation;
- Avoiding direct confrontation until the response process is established.

C. Preserve the process

Administrators should avoid taking steps that could compromise the district's legal, HR, forensic, or law enforcement response.

Administrators should not personally open files, direct staff to search for more content, interview the employee informally, question students, or share details with uninvolved personnel.

D. Involve counsel early

District legal counsel should be involved promptly when an alert may involve inappropriate sexual content, suspected child exploitation, student safety concerns, employee misconduct, possible criminal exposure, credentialing consequences, potential litigation, or public communication risk.

4. What Administrators Should Not Do

Administrators should avoid well-intentioned actions that may create additional risk.

Administrators should not:

- Open, view, copy, screenshot, forward, or distribute suspicious content;
- Ask IT staff to "look around" without legal or forensic direction;
- Interview the employee before HR and counsel set the process;
- Question students or witnesses casually;

- Tell staff members who do not have a need to know;
- Allow gossip or speculation to spread internally;
- Promise confidentiality beyond what law or district policy allows;
- Delay mandated reporting because the district wants to confirm more facts;
- Allow the employee to continue accessing students, devices, accounts, or records if containment is warranted;
- Delete, rename, quarantine, or move files unless directed by counsel, law enforcement, or a qualified forensic examiner;
- Treat the matter as only an IT issue.

The California Department of Education states that school districts and county offices of education do not investigate child abuse allegations or attempt to contact the person suspected of abuse or neglect; those responsibilities belong to appropriate investigative agencies.

5. Mandated Reporting Awareness

Administrators should understand that some digital risk alerts may create or coincide with mandated reporting obligations.

A digital alert may require urgent escalation if it suggests:

- Child sexual abuse material;
- Child exploitation;
- Grooming or boundary violations;
- Sexual communication involving a student or minor;
- Abuse, neglect, coercion, or threats;
- Employee misconduct involving student safety;
- A student victim or potential victim;
- An immediate risk to a child or school community.

For California matters involving suspected child abuse or neglect, the California DOJ's suspected child abuse report form states that mandated reporters must report to a designated agency immediately or as soon as practically possible by telephone and submit the written report within 36 hours of receiving the information.

Administrators should not impede, delay, or substitute themselves for a mandated reporter. Administrators may coordinate district response, but individual mandated reporters may still have their own reporting obligations.

6. Internal Coordination

Administrators should ensure the matter is routed to the correct internal functions without over-disclosing sensitive information.

HR coordination

HR should be involved when the alert involves an employee, contractor, substitute, volunteer, coach, intern, or other adult associated with the district.

HR may need to coordinate:

- Employee classification;
- Administrative leave;
- Access restrictions;
- Return of district property;
- Union or representation issues;
- Personnel documentation;
- Employee communication;
- Investigation procedures;
- Credentialing implications.

IT coordination

IT should be involved for preservation and access control, not informal investigation.

IT may need to coordinate:

- Device preservation;
- Account suspension or restriction;
- Log preservation;
- Asset information;
- Cloud-storage preservation;
- Email or network records;
- Alert metadata;
- Chain-of-custody documentation.

Legal counsel coordination

Legal counsel should help determine:

- Reporting obligations;
- Preservation instructions;
- Privilege protocols;
- Employee communication;
- Law enforcement coordination;
- Board communication;
- Parent/media communication;
- JPA or insurance notice;
- Public records and student privacy implications.

Site leadership coordination

If a principal or site administrator is involved, they should receive only the information necessary to protect students, manage site operations, and comply with district direction.

7. Student Safety Containment

Administrators should act promptly when student safety may be implicated, while avoiding actions that could compromise reporting or investigation.

Student safety containment may include:

- Removing the employee from student-facing contact;
- Adjusting supervision coverage;
- Securing classrooms, offices, devices, or storage areas;
- Preserving sign-in logs, schedules, seating charts, rosters, communication records, or camera footage;
- Ensuring students are not questioned without proper direction;
- Identifying whether any student may need immediate support;
- Coordinating with counseling or student services only as authorized and appropriate.

If student records or personally identifiable information may need to be shared during an emergency response, administrators should coordinate with counsel regarding FERPA. The U.S. Department of Education states that when a school discloses information under FERPA's health or safety emergency exception, it must record the articulable and significant threat that formed the basis for the disclosure and the parties to whom the information was disclosed.

8. Employee Access and Administrative Leave Coordination

Administrators should not independently decide employment action without HR and legal counsel unless district policy permits emergency action and immediate student safety requires it.

When appropriate, administrators should coordinate with HR and counsel regarding:

- Whether the employee should be placed on paid administrative leave;
- Whether the employee should be directed to leave campus;
- Whether the employee should be prohibited from contacting students;
- Whether the employee should be instructed not to access district systems;
- Whether district property should be collected;
- Whether building access should be suspended;
- Whether substitutes or coverage are needed;
- Whether a site-facing explanation is necessary.

Any communication with the employee should be neutral, factual, and reviewed by HR/counsel where possible.

Suggested administrative framing for review:

> "The District is reviewing a matter involving district technology use. While that review is pending, you are being directed not to access District systems, contact students, or return to District property unless authorized in writing."

9. Board Awareness

Administrators should coordinate with legal counsel before notifying the governing board or individual board members.

Board notification may be appropriate when the matter involves:

- Student safety;
- Employee misconduct;
- Potential litigation;
- Law enforcement involvement;
- Media or parent concern;
- Significant operational disruption;
- Credentialing implications;
- JPA, insurer, or risk-pool notice;
- A senior administrator or high-profile employee;
- Possible closed-session personnel or litigation issues.

Administrators should avoid sending detailed factual narratives, screenshots, file descriptions, or speculative conclusions to the board by email.

Board communications should generally be:

- Limited;
- Factual;
- Privileged where appropriate;
- Coordinated through counsel;
- Consistent with open-meeting and closed-session rules;
- Focused on process and safety, not rumor or premature conclusions.

Suggested board-facing framing for review:

> "The District is aware of a confidential personnel and technology-use matter. District leadership has taken steps to preserve records, protect student safety, involve legal counsel, and coordinate appropriate next steps. Additional information will be provided through the appropriate confidential process as permitted."

10. Parent, Staff, and Community Communication

Administrators should not communicate broadly until the district has coordinated with legal counsel, HR, and any involved investigative agencies.

Communication decisions may depend on:

- Whether students are directly involved;
- Whether law enforcement or child protective agencies are investigating;
- Whether parent notification is legally required or strategically appropriate;
- Whether FERPA or personnel confidentiality limits disclosure;
- Whether there is a safety concern requiring immediate notice;
- Whether media attention or public speculation has already started;
- Whether the district needs a holding statement.

Suggested holding statement for review:

> "The District is aware of a matter involving district technology use and has taken appropriate steps to preserve records, protect students, and involve the appropriate internal and external authorities. Because this matter may involve personnel, student privacy, and/or an active review, the District cannot provide additional details at this time."

This language should be reviewed by district counsel and communications leadership before use.

11. JPA, Insurance, and Risk-Pool Coordination

Administrators should coordinate with legal counsel and the district's risk manager to determine whether notice should be provided to the JPA, insurer, risk pool, or excess carrier.

Notice may be appropriate when the matter involves:

- Potential student harm;
- Employee misconduct;
- Possible civil liability;
- Law enforcement involvement;
- Media or community concern;
- Board-level concern;
- Employment litigation risk;
- Need for approved counsel, investigators, or forensic vendors;
- Potential claim preservation obligations.

Administrators should avoid assuming that a matter is too early or too uncertain for notice. Counsel and risk management should review applicable requirements.

12. Credentialing Awareness

If the employee is certificated, administrators should coordinate with HR, the superintendent's office, and legal counsel regarding whether credentialing reporting obligations may be implicated.

The California Commission on Teacher Credentialing states that employing school districts are required to report allegations of misconduct under specified California regulations and Education Code provisions, and its guidance states that superintendents must report a credential holder's change in employment status due to allegations of misconduct under CCR section 80303.

The CTC's section 80303 guidance states that the superintendent of an employing school district shall report a change in employment status to the Commission within 30 days after final employment action when a credential holder in a credentialed position experiences certain employment changes as a result of an allegation of misconduct or while an allegation is pending.

13. Documentation Protocol

Administrators should ensure that decisions and actions are documented clearly and chronologically.

Documentation should include:

- Date and time the alert was received;
- Who received the alert;
- Who was notified;
- Employee/user name and role;
- Device or account involved;
- Immediate safety steps taken;
- Access restrictions applied;
- Device preservation steps;
- HR involvement;
- Legal counsel involvement;
- Mandated reporting awareness or escalation;
- Law enforcement, CPS, CTC, JPA, insurer, or board notice, if applicable;
- Communication decisions;
- Next assigned action.

Documentation should avoid speculation, emotional language, or unsupported conclusions.

Preferred wording:

> "District administration was notified of a digital risk alert involving a district-managed device assigned to [employee/user]. The matter was escalated to HR, IT, and legal counsel. Access and preservation steps were initiated pending further direction."

Avoid wording such as:

> "Employee was caught with illegal material."

Unless an authorized determination has been made, administrative documentation should remain neutral and process-focused.

14. Administrator Checklist

Immediate Administrator Checklist

- Confirm receipt of the alert.
- Identify the employee/user, device, account, and location.
- Notify the designated district response lead.
- Involve HR, IT, and legal counsel.
- Limit internal knowledge to need-to-know personnel.
- Ensure suspicious content is not opened, copied, forwarded, deleted, or altered.
- Preserve the device, account, alert, and related logs.
- Determine whether immediate student-safety containment is needed.
- Coordinate employee access restrictions or administrative leave through HR/counsel.
- Confirm mandated reporting awareness and avoid interfering with any reporting obligation.
- Determine whether law enforcement, CPS, CTC, JPA, insurer, or board notice may be implicated.
- Avoid informal employee, student, or witness interviews.
- Prepare any parent, staff, board, or media communication only through approved channels.
- Document all actions taken.

15. Administrator Guiding Principle

The administrator's first job is not to prove what happened.

The administrator's first job is to create a safe, controlled, and defensible response path.

> **Protect students. Preserve evidence. Limit access. Involve the right people. Communicate carefully. Document every step.**

JPAs & Risk Managers Response Guide

JPA Coordination, District Consistency, Claim Awareness, and Risk Reduction

1. Purpose of This Guide

When inappropriate, high-risk, or potentially unlawful digital content is identified on a district-managed device, account, or network, the affected district may need to respond quickly across multiple lanes: student safety, HR, legal, technology, evidence preservation, mandated reporting, law enforcement coordination, communications, and potential claim exposure.

For JPAs, risk pools, and risk managers, the concern is not only whether the individual district responds. The concern is whether the district responds consistently, defensibly, and early enough to reduce harm, preserve evidence, and protect the integrity of any future claim, investigation, or administrative process.

This guide is intended to help JPAs, risk managers, claims personnel, and member-district support teams understand how to support districts after a digital risk alert without replacing district leadership, legal counsel, HR, mandated reporters, law enforcement, or child protective agencies.

This guide is not legal advice, insurance advice, claims-handling direction, forensic advice, law enforcement direction, or mandated reporting instruction.

JPA & Risk Manager Scope Note

This guide is provided for general coordination and risk-management planning purposes only. NetPropriate does not provide legal advice, insurance advice, coverage opinions, claims-handling direction, forensic advice, law enforcement direction, or mandated reporting instruction. NetPropriate does not determine whether a claim exists, whether coverage applies, whether abuse or misconduct occurred, whether content is criminal, or whether a specific report or notice must be made. All decisions involving claim notice, coverage, legal defense, student safety, employee access, mandated reporting, law enforcement contact, board notification, public communication, employment action, or external reporting should be made by the appropriate district officials, JPA/risk-pool representatives, legal counsel, insurers, mandated reporters, law enforcement, child protective agencies, or other authorized entities.

2. Role of the JPA or Risk Manager After an Alert

JPAs and risk managers are uniquely positioned to help districts avoid inconsistent, delayed, or improvised responses.

A JPA or risk manager may support the district by helping ensure:

- The district understands the seriousness of the alert;
- The correct internal response team is activated;
- Evidence and records are preserved;
- Legal counsel is involved early;
- Student safety considerations are addressed promptly;
- Claims notice requirements are evaluated;
- District communications remain careful and controlled;
- Member districts follow a consistent minimum response protocol;
- After-action review and training opportunities are captured.

California JPAs are commonly used by public agencies, including school districts, to pool resources for risk control and claims-related purposes. CAJPA describes JPAs as government-regulated public entities formed by public agencies, including school districts, that pool assets to promote risk control and pay claims against member entities.

California Government Code section 990.8 also addresses joint powers agreements involving pooling of self-insured claims or losses among public entities.

3. Immediate JPA / Risk Manager Priorities

When a member district reports a NetPropriate alert or other digital risk concern, the JPA or risk manager should focus first on stabilization, preservation, and proper routing.

A. Confirm the district has activated the correct response team

The JPA or risk manager should confirm that the district has involved, or is in the process of involving:

- Superintendent or designee;
- District legal counsel;
- HR director;
- IT director or technology lead;
- Site administrator, where appropriate;
- Claims/risk representative;
- Communications/public information officer, if needed;
- Law enforcement, CPS, or other external agency, when appropriate.

The JPA should not become the district's substitute decision-maker. The JPA's role is to support process integrity and ensure the district understands available risk-management resources.

B. Confirm preservation steps are underway

The JPA or risk manager should encourage the district to preserve relevant evidence and records, including:

- The district-managed device;
- User account information;
- Alert metadata;
- File path or hash-match information;
- Device serial number and asset tag;
- Assignment history;
- Network and login logs;
- Web-filtering logs, if applicable;
- Email and cloud-storage records;
- Relevant HR records;
- Acceptable Use Policy acknowledgments;
- Prior complaints, discipline, or related reports;
- Chain-of-custody documentation.

The district should avoid opening, copying, forwarding, deleting, renaming, moving, or further investigating suspicious files unless directed by legal counsel, law enforcement, or a qualified forensic examiner.

C. Encourage early counsel involvement

The JPA or risk manager should encourage the member district to involve legal counsel early, particularly where the alert may involve:

- Student safety;
- Employee misconduct;
- Suspected child exploitation;
- Suspected child sexual abuse material;
- Criminal exposure;
- Credentialing implications;
- Potential civil liability;
- Media exposure;

- Parent/community concern;
- Possible board notification;
- Employment discipline or separation.

D. Evaluate claims or coverage notice

The JPA or risk manager should determine whether the alert may trigger internal notice, claim reporting, coverage review, excess carrier notice, panel counsel assignment, forensic vendor approval, or risk-pool involvement.

The district should not wait until a lawsuit, demand letter, media inquiry, or law enforcement action occurs before evaluating notice requirements.

4. Why Consistency Matters Across Member Districts

Inconsistent response can create avoidable risk.

Two districts may face similar alerts, but if one preserves evidence, involves counsel, limits access, and documents decisions while another delays, investigates informally, or allows continued access, the legal and claims posture may be very different.

JPAs and risk managers can help standardize the minimum response expectations across member districts, including:

- Who receives alerts;
- Who must be notified internally;
- When counsel is involved;
- When HR is involved;
- When IT preserves rather than investigates;
- When the JPA/risk pool should be notified;
- What records should be preserved;
- What actions should be avoided;
- How chain of custody should be documented;
- How board or media communications should be controlled;
- How post-incident review should occur.

The goal is not to remove district discretion. The goal is to prevent districts from improvising during high-pressure moments.

5. Recommended Member-District Minimum Response Protocol

JPAs may consider encouraging member districts to adopt a minimum protocol for digital risk alerts.

A minimum protocol may include:

Step 1: Acknowledge and preserve

The district confirms receipt of the alert and immediately preserves the device, account, alert information, and relevant logs.

Step 2: Limit access

The district limits unnecessary access to suspicious content and determines whether employee system access, building access, or student contact should be restricted.

Step 3: Notify the internal response team

The district notifies the appropriate internal response personnel, typically including superintendent/designee, HR, IT, legal counsel, and site leadership where appropriate.

Step 4: Evaluate reporting obligations

The district, counsel, and mandated reporters evaluate whether mandated reporting, law enforcement contact, CPS notification, NCMEC reporting, CTC reporting, Title IX procedures, or other external reporting may be implicated.

In California, mandated reporters must report known or suspected child abuse or neglect, and the CDE states it is not the mandated reporter's role to determine whether the allegation is valid before reporting. California DOJ materials state that mandated reporters generally must make the initial telephone report immediately or as soon as practicably possible and submit the written report within 36 hours.

Step 5: Notify the JPA/risk pool as appropriate

The district or counsel evaluates whether the JPA, risk pool, insurer, or excess carrier should receive notice.

Step 6: Document every action

The district maintains a chronological record of actions taken, decisions made, people notified, records preserved, and external contacts completed.

6. Claim Awareness and Notice Considerations

Digital risk alerts may not immediately look like claims, but they can become claims.

A JPA or risk manager should evaluate whether the matter may involve:

- Potential student harm;
- Employee sexual misconduct;
- Failure-to-supervise allegations;
- Negligent hiring, retention, or supervision claims;
- Title IX exposure;
- Civil rights allegations;
- Failure to report;
- Failure to preserve evidence;
- Employment litigation;
- Wrongful termination or discipline;
- Credentialing consequences;
- Public records or privacy disputes;
- Media or reputational harm;
- Law enforcement investigation;
- Future demand letter or lawsuit.

The JPA or risk manager should review applicable memoranda of coverage, claims-reporting provisions, excess coverage requirements, defense-counsel rules, approved investigator lists, forensic-vendor requirements, and any timing requirements for notice.

7. Evidence Preservation and Chain of Custody

JPAs and risk managers should encourage member districts to preserve evidence before anyone attempts to interpret, explain, minimize, or "confirm" the alert.

Preservation may include:

- Physical custody of the device;
- Secure storage location;
- Device condition at time of collection;
- Device serial number and asset tag;
- Assigned user;
- Date and time of collection;
- Person collecting the device;

- Person receiving the device;
- Account status;
- Login/session data;
- Cloud-storage access;
- Relevant logs;
- Alert metadata;
- Prior technology-use records.

A simple chain-of-custody log should document every transfer or access event.

At minimum, the log should include:

- Date;
- Time;
- Item/device/account;
- Description;
- Serial number or identifier;
- Released by;
- Received by;
- Purpose of transfer;
- Storage location;
- Notes.

The district should avoid unnecessary access to suspected unlawful content. In matters involving suspected child sexual abuse material or child exploitation, districts should involve legal counsel and appropriate authorities before further review or handling.

8. Coordination With District Legal Counsel

The JPA or risk manager should avoid giving legal instructions directly to the district unless authorized to do so within the JPA's structure and in coordination with counsel.

Instead, the JPA or risk manager should help ensure that district counsel is addressing key questions, including:

- Has the device and account been preserved?
- Has unnecessary access to content been stopped?
- Has HR been involved?
- Has student safety containment been considered?
- Has mandated reporting been evaluated?
- Has law enforcement or CPS involvement been considered?
- Has CTC reporting been considered for certificated employees?
- Has the JPA/risk pool received timely notice?
- Is there a need for panel counsel, outside investigator, or forensic examiner?
- Are communications being controlled?
- Are board, parent, staff, or media communications being reviewed?
- Are public records and student privacy issues implicated?

The JPA's value is in making sure the right questions are asked before avoidable mistakes occur.

9. Coordination With HR, IT, and Administration

A digital risk alert is rarely just an IT issue.

The JPA or risk manager should encourage role clarity across the district response team.

HR should generally handle:

- Employment status;

- Administrative leave;
- Employee communication;
- Union or representation issues;
- Personnel documentation;
- Return of district property;
- Credentialing coordination;
- Employee discipline process.

IT should generally handle:

- Device preservation;
- Account containment;
- Log preservation;
- Asset records;
- Technical information;
- Access control;
- Support for forensic preservation.

Administration should generally handle:

- Student safety;
- Site operations;
- Internal coordination;
- Board awareness;
- Communications discipline;
- Parent/community escalation, if needed.

Legal counsel should generally handle:

- Legal strategy;
- Privilege;
- Reporting analysis;
- Law enforcement coordination;
- Evidence-preservation direction;
- Employment/legal risk;
- Claim and coverage coordination;
- Communications review.

The JPA should support the structure, not blur the lanes.

10. High-Severity Alert Triage

Some alerts should be treated as potentially high-severity from the outset.

High-severity factors may include:

- Suspected child sexual abuse material;
- Suspected child exploitation;
- Student victim or potential student victim;
- Grooming or boundary-violation indicators;
- Sexual communication involving a student or minor;
- Threats, coercion, stalking, sextortion, or violence;
- Employee in a trusted-access or student-facing role;
- Prior complaints or warning signs;
- Multiple devices or accounts implicated;
- Attempted deletion, concealment, encryption, or evasion;

- Media, parent, board, or law enforcement awareness.

For suspected online child exploitation, NCMEC describes the CyberTipline as the national centralized reporting system for suspected online exploitation of children, including child sexual abuse material, online enticement, child sex trafficking, and related concerns.

A high-severity alert should generally trigger urgent coordination with district leadership, counsel, HR, IT, and appropriate external authorities.

11. Communications and Reputation Risk

JPAs and risk managers should help districts understand that communications can create risk even when the district is trying to reassure the community.

Communication risks may include:

- Overstating facts;
- Disclosing student information;
- Disclosing personnel information;
- Undermining an active investigation;
- Making inconsistent statements across administrators;
- Creating admissions of liability;
- Minimizing concerns prematurely;
- Failing to acknowledge student-safety steps;
- Allowing rumors to fill the silence.

Suggested district holding language for counsel review:

> "The District is aware of a matter involving district technology use and has taken appropriate steps to preserve records, protect students, and involve the appropriate internal and external authorities. Because this matter may involve personnel, student privacy, and/or an active review, the District cannot provide additional details at this time."

JPAs should encourage districts to have counsel review parent, board, staff, public, and media communications before release.

12. Common District Response Mistakes

JPAs and risk managers should train member districts to avoid common mistakes that can increase risk.

Districts should not:

- Treat the alert as a routine IT ticket;
- Open suspicious files to "confirm" what they are;
- Forward suspected content by email;
- Ask IT staff to search broadly without direction;
- Allow the assigned employee continued access when containment is warranted;
- Delay legal counsel involvement;
- Delay mandated reporting because the district wants more certainty;
- Interview students, staff, or the employee casually;
- Over-disclose to board members, staff, or community members;
- Delete, quarantine, rename, or move files without direction;
- Fail to document actions taken;
- Wait too long to notify the JPA, risk pool, or insurer;
- Enter into separation terms that interfere with required reporting, disclosure, or record retention.

The most dangerous response pattern is often not malicious. It is a well-intentioned district trying to "figure it out internally" before involving the right people.

13. JPA Training and Tabletop Exercises

JPAs can add significant value by helping member districts practice before an actual incident occurs.

Training may include:

- Annual digital risk response training;
- HR/legal/IT/admin role-mapping;
- Mandated reporting refreshers;
- Evidence-preservation basics;
- Chain-of-custody practice;
- Communications drills;
- Board-notification scenarios;
- JPA notice requirements;
- Mock high-severity alert response;
- Post-incident debrief procedures.

A tabletop exercise should test whether the district can answer:

- Who receives the alert?
- Who is contacted first?
- Who calls legal counsel?
- Who preserves the device?
- Who controls employee access?
- Who determines administrative leave?
- Who evaluates mandated reporting?
- Who notifies the JPA or insurer?
- Who communicates with the board?
- Who communicates with parents or media?
- Who documents the timeline?

A district should not be discovering those answers during a crisis.

14. Recommended JPA Resource Packet for Member Districts

JPAs may consider maintaining a standardized packet for member districts that includes:

- Immediate Response Checklist;
- HR Response Guide;
- Legal Counsel Guide;
- Administrator Guide;
- Evidence Preservation Guide;
- CSAM / Child Exploitation Escalation Guide;
- Chain-of-Custody Log;
- Incident Timeline Template;
- JPA Notice Checklist;
- Board/Media Holding Statement Template;
- Post-Incident Review Worksheet;
- Tabletop Exercise Scenario.

This creates a consistent foundation while still allowing each district and its counsel to adapt the response to local policy, bargaining agreements, coverage requirements, and facts.

15. Post-Incident Review

After the immediate matter stabilizes, the JPA or risk manager should encourage a structured post-incident review.

The review should evaluate:

- How quickly the alert was received and escalated;
- Whether the correct people were notified;
- Whether evidence was preserved properly;
- Whether employee access was contained appropriately;
- Whether mandated reporting was considered or completed;
- Whether counsel was involved early enough;
- Whether JPA/insurer notice was timely;
- Whether communications were controlled;
- Whether any policy gaps were identified;
- Whether training or tabletop exercises are needed;
- Whether technology, HR, or documentation protocols should be revised.

The purpose is not blame. The purpose is risk reduction and response improvement.

16. JPA / Risk Manager Checklist

Immediate JPA / Risk Manager Checklist

- Confirm the member district has received and acknowledged the alert.
- Confirm the matter has been escalated to district leadership.
- Confirm HR, IT, and legal counsel are involved or being contacted.
- Encourage preservation of the device, account, alert, and logs.
- Confirm the district understands not to open, copy, forward, delete, rename, or alter suspicious content.
- Determine whether the matter may trigger claim, coverage, JPA, insurer, or excess carrier notice.
- Confirm whether student safety containment is being evaluated.
- Confirm whether employee access restrictions or administrative leave are being reviewed by HR/counsel.
- Confirm mandated reporting awareness without interfering with individual reporting obligations.
- Confirm whether law enforcement, CPS, NCMEC, CTC, or other external reporting may be implicated.
- Determine whether approved counsel, investigator, or forensic vendor involvement is needed.
- Encourage careful, counsel-reviewed communications.
- Begin a JPA/risk file or internal incident record as appropriate.
- Track timeline, decisions, and follow-up items.
- Schedule post-incident review after immediate stabilization.

17. JPA / Risk Manager Guiding Principle

A digital risk alert is not only a technology event. It may become a student-safety event, employment matter, legal matter, claim event, public-relations issue, or criminal investigation.

The JPA's role is to help member districts avoid improvisation.

> **Standardize the response. Preserve the record. Protect students. Support counsel. Reduce preventable risk. Document every step.**

Evidence Preservation Response Guide

What Not to Touch, What to Preserve, and How to Protect Chain of Custody

1. Purpose of This Guide

When inappropriate, high-risk, or potentially unlawful digital content is identified on a district-managed device, account, or network, the first response can significantly affect the integrity of any later administrative review, HR process, legal analysis, law enforcement referral, forensic examination, insurance claim, or civil proceeding.

This guide is intended to help districts, JPAs, legal counsel, HR teams, administrators, IT personnel, and other authorized response personnel understand basic evidence-preservation principles after a digital risk alert.

The goal is not to conduct a full forensic investigation internally. The goal is to prevent unnecessary handling, preserve relevant records, maintain a clear chain of custody, and allow the appropriate legal, forensic, administrative, or law enforcement process to proceed without avoidable contamination.

Evidence Preservation Scope Note

This guide is provided for general preservation-awareness and planning purposes only. NetPropriate does not provide forensic advice, legal advice, law enforcement direction, mandated reporting instruction, evidence-handling certification, or investigative direction. NetPropriate does not determine whether content is criminal, whether evidence is admissible, whether a device should be imaged, whether law enforcement should seize a device, or whether a specific report must be made. All decisions involving evidence handling, forensic imaging, chain of custody, law enforcement contact, mandated reporting, employee discipline, student safety, legal holds, insurance/JPA notice, or external reporting should be made by the appropriate district officials in coordination with legal counsel, qualified forensic professionals, JPAs/risk pools, insurers, mandated reporters, law enforcement, child protective agencies, or other authorized entities.

2. Evidence Preservation Guiding Principle

After a digital risk alert, the safest first response is usually:

Stop. Preserve. Limit access. Document. Escalate.

Personnel should avoid curiosity-driven review. Opening files, forwarding screenshots, copying suspected material, deleting files, moving folders, or allowing the assigned user to continue using the device may create unnecessary risk.

The district's first preservation objective is to maintain the condition of the device, account, alert data, and related records as close as possible to the state in which they existed when the alert was identified.

3. Immediate Preservation Priorities

Upon receiving a NetPropriate alert or other digital risk notice, the district should promptly identify and preserve relevant information.

Immediate preservation priorities may include:

- The district-managed device;
- The assigned user account;
- The NetPropriate alert record;
- File path, hash-match, or alert metadata;
- Device serial number and asset tag;
- Device assignment history;

- Login and authentication records;
- Network access logs;
- Web-filtering logs, if applicable;
- Email and cloud-storage records;
- Local user profile information;
- Backup or snapshot records;
- Acceptable Use Policy acknowledgments;
- Prior technology-use reports or complaints;
- HR/personnel records, where relevant;
- Chain-of-custody documentation.

4. What Personnel Should Not Do

Well-intentioned internal review can unintentionally compromise evidence or create additional legal exposure.

Personnel should not:

- Open suspicious files to “see what they are”;
- Preview images or videos out of curiosity;
- Copy files to a thumb drive, desktop folder, cloud location, or email;
- Forward screenshots, filenames, images, videos, or file samples;
- Delete, quarantine, rename, move, or alter suspicious files;
- Ask IT to search broadly without counsel-directed parameters;
- Continue using the device for normal work;
- Allow the assigned user to retain access to the device or account if containment is warranted;
- Run cleanup tools, antivirus remediation, or system updates without direction;
- Restart, wipe, reimage, reset, or redeploy the device unless directed;
- Change passwords or terminate sessions without considering preservation impact;
- Discuss alert details with staff who do not have a need to know;
- Document conclusions before the facts are reviewed by appropriate authorities.

The objective is to preserve the evidence, not to prove the alert through informal internal review.

5. Device Preservation

When a device is associated with an alert, the district should preserve the device and prevent unnecessary use.

Device preservation may include:

- Identifying the physical device;
- Recording the device type, make, model, serial number, and asset tag;
- Identifying the assigned user;
- Recording the date and time the device was located;
- Photographing the exterior condition of the device, if appropriate;
- Documenting whether the device was powered on, asleep, locked, connected to power, or connected to a network;
- Limiting access to authorized personnel;
- Securing the device in a locked location;
- Waiting for counsel, law enforcement, or forensic direction before imaging, powering down, disconnecting, or manipulating the device.

Whether to leave a device powered on, power it down, disconnect it from the network, or capture volatile memory can be fact-specific. Those decisions should be made with legal counsel, qualified forensic personnel, or law enforcement when appropriate.

6. Account and Cloud Preservation

Digital evidence may not live only on the physical device. Relevant information may also exist in cloud systems, email platforms, browser sync, shared drives, learning platforms, identity systems, security tools, or backup environments.

The district should consider preserving:

- Email accounts;
- Cloud storage accounts;
- Browser sync data;
- File-sharing records;
- Learning management system access;
- Student information system access logs;
- Authentication/MFA logs;
- VPN logs;
- Web-filtering records;
- Endpoint security logs;
- Backup or retention snapshots;
- Admin audit logs;
- Shared drive permissions;
- Account assignment and access history.

Account restrictions should be coordinated carefully. For example, disabling an account may be appropriate for containment, but the district should consider whether doing so affects logs, sessions, retention settings, or cloud evidence.

Legal counsel and IT should coordinate before account changes are made.

7. Log Preservation

Logs can be highly time-sensitive. Some systems overwrite, rotate, or age out logs after a short retention period.

The district should identify which logs may be relevant and preserve them promptly.

Potential logs may include:

- Device login logs;
- Network authentication logs;
- VPN logs;
- Web-filtering logs;
- Firewall logs;
- Endpoint detection logs;
- Email audit logs;
- Cloud storage access logs;
- File creation, modification, or access timestamps;
- Browser history or sync records, where available and legally appropriate;
- Identity provider logs;
- MFA logs;
- Print logs;
- Remote-access logs;
- Administrative action logs.

The district should document who preserved the logs, when they were preserved, where they were stored, and whether the preserved copy is complete.

8. Chain of Custody

Chain of custody is the documented history of who had possession or control of evidence, when they had it, why they had it, and what happened to it.

For digital risk alerts, chain-of-custody documentation should begin as soon as the device, account, alert, or related record is preserved.

A chain-of-custody log should include:

- Date;
- Time;
- Item or evidence description;
- Device serial number, asset tag, account name, or record identifier;
- Location found;
- Condition when found;
- Person releasing the item or record;
- Person receiving the item or record;
- Reason for transfer;
- Storage location;
- Access restrictions;
- Notes regarding any handling, copying, imaging, or review;
- Signature or acknowledgment, where appropriate.

If an item changes hands, the log should be updated every time.

9. Alert Record Preservation

The NetPropriate alert itself should be preserved as part of the district's response record.

The preserved alert record may include:

- Alert date and time;
- Recipient of the alert;
- User or device associated with the alert;
- Device identifier;
- File path or location information, where available;
- Hash-match information, where available;
- Alert category or severity;
- Any automated system metadata;
- District response actions;
- Personnel notified;
- Preservation steps taken;
- Follow-up actions assigned.

The alert record should be preserved without expanding unnecessary access to suspected content.

If the alert involves hash-matched or otherwise flagged material, personnel should avoid attempting to independently open or verify the underlying content unless directed by counsel, law enforcement, or a qualified forensic examiner.

10. Suspected CSAM or Child Exploitation Concerns

If an alert may involve suspected child sexual abuse material, child exploitation, online enticement, child sex trafficking, or unlawful sexual content involving minors, the district should treat the matter as high severity.

Personnel should not open, copy, forward, screenshot, transmit, or distribute suspected material.

The appropriate response may include immediate coordination with:

- District legal counsel;
- Mandated reporters;
- Law enforcement;
- Child protective agencies;
- NCMEC CyberTipline;
- Qualified forensic professionals;
- JPA/risk pool or insurer, where applicable.

11. Role Clarity During Preservation

Evidence preservation requires clear lanes.

IT's role

IT may assist with:

- Identifying devices;
- Restricting access;
- Preserving logs;
- Maintaining asset records;
- Exporting system metadata;
- Supporting forensic preservation;
- Documenting technical steps taken.

IT should not be asked to conduct an informal criminal investigation or independently determine whether content is unlawful.

HR's role

HR may assist with:

- Employee access restrictions;
- Administrative leave coordination;
- Personnel record preservation;
- Policy acknowledgment records;
- Employee communication;
- Union or representation coordination.

HR should avoid characterizing the evidence or drawing conclusions before appropriate review.

Administration's role

Administrators may assist with:

- Student safety containment;
- Site operations;
- Internal coordination;
- Board awareness;
- Communications discipline;
- Ensuring the right personnel are involved.

Administrators should avoid broad disclosure or informal witness questioning.

Legal counsel's role

Legal counsel may assist with:

- Preservation instructions;
- Privilege protocols;
- Reporting analysis;

- Law enforcement coordination;
- Forensic examiner engagement;
- HR and employment coordination;
- JPA/insurance notice;
- Communications review.

12. Forensic Imaging and Examination

Forensic imaging or deeper examination should generally be handled by qualified forensic personnel or law enforcement when appropriate.

The district should not assume that ordinary IT copying, drag-and-drop duplication, screenshots, or manual file review will preserve evidence properly.

Depending on the circumstances, counsel or law enforcement may determine whether to:

- Preserve the device without further action;
- Create a forensic image;
- Capture volatile memory;
- Preserve cloud records;
- Export logs;
- Use an outside forensic examiner;
- Transfer the device to law enforcement;
- Maintain the device in district custody pending direction.

These decisions are fact-specific and should be documented.

13. Communications About Evidence

Personnel should avoid unnecessary written commentary about suspected evidence.

Written communications should be factual, limited, and process-focused.

Preferred wording:

> "A digital risk alert was received involving a district-managed device. The device, alert record, and related access information are being preserved pending further direction from district leadership and counsel."

Avoid wording such as:

> "We found illegal material on the employee's laptop."

Unless an authorized determination has been made, records should avoid legal conclusions, inflammatory descriptions, speculation, or assumptions about intent.

Personnel should also avoid sending detailed descriptions of suspected content to broad email groups, board members, staff, or anyone without a defined response role.

14. Storage and Access Control

Preserved devices and records should be stored securely.

Storage and access-control practices may include:

- Locked physical storage;
- Limited key or badge access;
- Restricted digital folders;
- Access logs;
- No shared passwords;
- No informal copying;

- No personal cloud storage;
- No use of personal devices;
- No forwarding to private email accounts;
- No removal from district custody without documentation;
- Separate privileged or counsel-directed folders where appropriate.

Only authorized personnel should access preserved evidence, and each access should be documented when the evidence itself is touched, transferred, copied, imaged, or reviewed.

15. Preservation Timeline

A simple preservation timeline should be maintained from the first alert forward.

The timeline should include:

- When the alert was received;
- Who received it;
- Who was notified;
- When the device was located;
- Who had possession of the device;
- Whether the device was powered on, locked, connected, or in use;
- When account access was restricted;
- When logs were preserved;
- When counsel was contacted;
- When HR was contacted;
- When JPA/insurer notice was considered or completed;
- When law enforcement, CPS, NCMEC, CTC, or other agencies were contacted, if applicable;
- When any forensic examiner was engaged;
- When any transfer, imaging, review, or storage action occurred.

The timeline should be factual and should avoid speculation.

16. Common Evidence Preservation Mistakes

Districts should train personnel to avoid common mistakes, including:

- Treating the alert as a routine helpdesk issue;
- Allowing multiple people to inspect the device;
- Opening files to confirm the alert;
- Forwarding screenshots or suspected files;
- Deleting or quarantining material without direction;
- Continuing to use the device;
- Reassigning or reimaging the device too quickly;
- Failing to preserve cloud records or logs;
- Forgetting to document chain of custody;
- Allowing the assigned user to retain access when containment is warranted;
- Discussing suspected content broadly;
- Failing to involve counsel early;
- Waiting too long to preserve logs;
- Using imprecise or inflammatory language in emails.

The safest approach is to preserve first and investigate only through the proper channel.

17. Evidence Preservation Checklist

Immediate Evidence Preservation Checklist

- Confirm receipt of the alert.
- Identify the device, account, user, and location.
- Preserve the alert record and metadata.
- Do not open, copy, forward, delete, move, rename, or alter suspicious content.
- Secure the device and prevent further use.
- Record the device serial number, asset tag, condition, and assigned user.
- Document whether the device is powered on, asleep, locked, connected, or offline.
- Notify legal counsel and designated district leadership.
- Coordinate with HR regarding employee access and device recovery.
- Preserve relevant account, cloud, authentication, network, and web-filtering logs.
- Restrict access to preserved records.
- Begin a chain-of-custody log.
- Document every transfer, access event, preservation step, and decision.
- Determine whether forensic imaging or law enforcement handling is needed.
- Evaluate whether mandated reporting, NCMEC, CPS, CTC, JPA, insurer, or other notice may be implicated.
- Avoid broad internal communication or speculative written conclusions.

18. Evidence Preservation Guiding Principle

Evidence preservation is not about doing more.

It is about preventing the wrong thing from being done too soon.

> **Do not touch what does not need to be touched. Preserve what may matter. Document who handled it. Escalate to the right authority. Keep the record clean.**

Disclaimer and Use of Materials

The NetPropriate Digital Risk Response Packet and related response guides are provided for general informational, educational, and planning purposes only. These materials are designed to help school districts, county offices of education, charter schools, joint powers authorities, risk pools, human resources teams, administrators, legal counsel, technology teams, and other authorized personnel think through practical response considerations when inappropriate, high-risk, or potentially unlawful digital content is identified on a district-managed device, account, or network.

These materials do not constitute legal advice, investigative advice, employment advice, forensic advice, law enforcement direction, insurance advice, or mandated reporting instruction. Use of these materials does not create an attorney-client relationship, investigator-client relationship, consultant-client relationship, or any other professional relationship with NetPropriate, its employees, contractors, representatives, or affiliates.

Districts, JPAs, and other organizations should consult their own legal counsel, governing policies, collective bargaining agreements, insurance/risk-pool requirements, law enforcement contacts, child protective agencies, and applicable federal, state, and local laws before taking action. Where applicable, users should also follow all mandated reporting obligations, credentialing-reporting requirements, personnel procedures, evidence-preservation requirements, privacy obligations, and student-safety protocols.

NetPropriate does not determine whether content is criminal, whether child abuse or exploitation has occurred, whether an employee has violated law or policy, whether discipline is appropriate, or whether any specific report must be made to law enforcement, child protective services, credentialing authorities, insurers, JPAs, or other agencies. Those determinations should be made by the appropriate district officials, legal counsel, mandated reporters, law enforcement agencies, child protective agencies, courts, or other authorized entities.

The guidance provided in these materials is not exhaustive and may not apply to every situation, jurisdiction, employee classification, bargaining-unit relationship, or factual circumstance. Laws, regulations, reporting duties, district policies, forensic practices, and agency procedures may change over time. Organizations are responsible for ensuring that their response practices are current, lawful, policy-compliant, and appropriate for the specific facts involved.

Nothing in these materials should be interpreted as permission to access, view, copy, transmit, distribute, alter, delete, or further investigate suspected unlawful content without proper legal, forensic, administrative, or law enforcement direction. In matters involving suspected child sexual abuse material, child exploitation, abuse, threats, or other urgent safety concerns, organizations should promptly involve appropriate legal counsel, mandated reporters, law enforcement, child protective agencies, or other authorized response entities as required.

NetPropriate provides technical detection, alerting, and response-support resources within the scope of its services. NetPropriate does not replace the judgment, duties, or responsibilities of school districts, JPAs, administrators, HR professionals, legal counsel, mandated reporters, law enforcement, child protective agencies, forensic examiners, insurers, or governing boards.

By using these materials, the reader acknowledges that they are responsible for applying their own policies, legal obligations, professional judgment, and authorized response procedures to the specific circumstances presented.