NetPropriate®
DISCOVER HIDDEN DIGITAL RISK | FIND PREDATORY BEHAVIOR

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.**

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.