NetPropriate®
DISCOVER HIDDEN DIGITAL RISK | FIND PREDATORY BEHAVIOR

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.**

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.