NetPropriate®
DISCOVER HIDDEN DIGITAL RISK | FIND PREDATORY BEHAVIOR

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.**

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.