NetPropriate®
DISCOVER HIDDEN DIGITAL RISK | FIND PREDATORY BEHAVIOR

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.**

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.