

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.

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.