Notification & Escalation Tracker

Internal and External Notification Documentation

1. Purpose of This Tracker

Use this tracker to document who was notified, when notification occurred, who made the notification, what method was used, and what follow-up remains after a digital risk alert involving a district-managed device, account, or network. This tracker is intended to support clear documentation and response coordination; it does not determine whether any report, notice, or external escalation is legally required.

Notification & Escalation Scope Note

This tracker is provided for general documentation and response-tracking purposes only. NetPropriate does not provide legal advice, law enforcement direction, employment advice, insurance advice, claims-handling direction, mandated reporting instruction, or investigative direction. This tracker documents notifications considered or completed; it does not determine whether a specific report, notice, employment action, public communication, or external escalation is legally required. All decisions 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. Incident Identification

Field	Response
Incident / matter name	
Date alert received	
Time alert received	
Initial alert source	☐ NetPropriate alert ☐ Internal report ☐ IT discovery ☐ Other: _____
Assigned user / employee	
Device / account involved	
Site / department	
Response lead	
Tracker started by	
Date/time tracker started	

3. Internal District Notification Tracker

Document internal notifications and coordination. Limit details to personnel with a legitimate need to know.

Role / Team	Needed?	Notified?	Date/Time	Notified By	Method / Contact	Notes / Follow-Up
HR	☐ Yes ☐ No ☐ Pending	☐ Yes ☐ No				
Legal counsel	☐ Yes ☐ No ☐ Pending	☐ Yes ☐ No				
Superintendent/designee	☐ Yes ☐ No ☐ Pending	☐ Yes ☐ No				
IT / technology lead	☐ Yes ☐ No ☐ Pending	☐ Yes ☐ No				
Site administrator	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No				
Communications / PIO	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No				
Safety / threat assessment team	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No				

4. JPA / Insurance Notification Tracker

Use this section to track JPA, risk-pool, insurer, or excess carrier notification review and completion. Notice requirements should be reviewed with legal counsel and the appropriate risk-management contacts.

Entity / Contact	Notice Reviewed?	Notified?	Date/Time	Notified By	Claim / Reference No.	Notes / Follow-Up
JPA / risk pool	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
Insurer / carrier	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
Excess carrier	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
Panel counsel / approved counsel	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
Approved investigator / forensic vendor	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				

5. External Reporting / Escalation Tracker

This section documents whether external reporting or escalation paths were reviewed or contacted. It does not determine whether a report is legally required. Individual mandated reporters may have separate obligations that are not satisfied by internal notification alone.

Escalation Path	Reviewed?	Contacted?	Date/Time	Person Responsible	Contact / Report No.	Notes / Follow-Up
Law enforcement	☐ Yes ☐ No ☐ Pending	☐ Yes ☐ No ☐ N/A				
Child protective agency / CPS	☐ Yes ☐ No ☐ Pending	☐ Yes ☐ No ☐ N/A				
NCMEC CyberTipline	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
California Commission on Teacher Credentialing / CTC	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
Title IX / student-safety process	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				
Other agency / authority	☐ Yes ☐ No ☐ Pending ☐ N/A	☐ Yes ☐ No ☐ N/A				

6. Board / Parent / Media Communication Decision Tracker

Use this section to document whether sensitive communications were considered, approved, delayed, or declined. Communications should be reviewed through the appropriate district process and legal counsel where applicable.

Communication Area	Status	Date/Time	Reviewed / Approved By	Sender / Speaker	Notes / Follow-Up
Board notification	☐ Pending ☐ Approved ☐ Delayed ☐ Not needed				
Parent/guardian communication	☐ Pending ☐ Approved ☐ Delayed ☐ Not needed				
Staff communication	☐ Pending ☐ Approved ☐ Delayed ☐ Not needed				
Media response	☐ Pending ☐ Approved ☐ Delayed ☐ Not needed				
Community/public statement	☐ Pending ☐ Approved ☐ Delayed ☐ Not needed				
Website/social media response	☐ Pending ☐ Approved ☐ Delayed ☐ Not needed				

7. Detailed Notification Log

Use this section for additional chronological notification entries, including return calls, follow-up emails, updated instructions, or delayed/pending decisions.

Date	Time	Person / Entity	Notification Type	Method	Completed By	Notes / Next Step
		HR				
		Legal counsel				
		Superintendent/designee				
		IT				
		JPA/risk pool				
		Law enforcement / CPS / NCMEC / CTC review				
		Board / parent / media decision				

8. Pending Notification Items

Pending Item	Responsible Person	Due Date/Time	Reason Pending	Completion Notes

9. Tracker Review and Sign-Off

Field	Response
Tracker reviewed by	
Title / role	
Date reviewed	
Time reviewed	
Known notification gaps	
Follow-up owner	
Next review date/time, if applicable	

10. Notification Reminder

This tracker documents notification activity. It does not replace mandated reporting, law enforcement coordination, legal review, JPA/insurance notice requirements, or district-specific communication approval processes.

Document who was notified, when they were notified, who notified them, and what follow-up remains.

Disclaimer and Use of Materials

The NetPropriate Digital Risk Response Packet and related response guides, forms, logs, and templates are provided for general informational, educational, documentation, 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, claims-handling direction, 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, whether evidence is admissible, 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.