

Post-Incident Review Worksheet

Response Debrief, Lessons Learned, and Procedure Improvement

1. Purpose of This Worksheet

Use this worksheet after the immediate response has stabilized to review what occurred, what worked, what was delayed, what was unclear, and what should be improved before a future digital risk alert. The purpose is not to assign blame. The purpose is to improve response consistency, preservation discipline, communication control, training readiness, and risk reduction.

Post-Incident Review Scope Note

This worksheet is provided for general debriefing, documentation, and planning purposes only. NetPropriate does not provide legal advice, forensic advice, law enforcement direction, insurance advice, claims-handling direction, employment advice, mandated reporting instruction, or investigative direction. This worksheet does not determine whether a response was legally sufficient, whether evidence was admissible, whether reporting obligations were satisfied, or whether discipline or policy changes are required. All conclusions, corrective actions, and procedure updates should be reviewed by the appropriate district officials in coordination with legal counsel, HR, IT, JPAs/risk pools, insurers, qualified forensic professionals, law enforcement, child protective agencies, or other authorized entities as appropriate.

2. Incident Identification

Field	Response
Incident / matter name	
Date alert received	
Date immediate response stabilized	
Review date	
Review facilitator	
Participating roles / departments	<input type="checkbox"/> HR <input type="checkbox"/> Legal counsel <input type="checkbox"/> IT <input type="checkbox"/> Administration <input type="checkbox"/> Site leadership <input type="checkbox"/> JPA/risk pool <input type="checkbox"/> Other: _____
Device / account involved	
Assigned user / employee	
Site / department	
Related logs/forms reviewed	<input type="checkbox"/> Intake Form <input type="checkbox"/> Timeline Log <input type="checkbox"/> Chain-of-Custody Log <input type="checkbox"/> Access Restriction Checklist <input type="checkbox"/> Notification Tracker <input type="checkbox"/> Other: _____

3. What Went Well

Document response actions, decisions, communications, or coordination points that worked effectively and should be preserved in future procedures.

Area Reviewed	What Went Well	Evidence / Example	Keep / Repeat?
Alert receipt and routing			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Needs revision
Initial stabilization			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Needs revision
Evidence preservation			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Needs revision
Access containment			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Needs revision
HR/legal/IT coordination			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Needs revision

Area Reviewed	What Went Well	Evidence / Example	Keep / Repeat?
Communication control			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Needs revision

4. What Was Delayed

Identify delays that affected preservation, escalation, access containment, reporting review, communications, or decision-making.

Delayed Item	Expected Timing	Actual Timing	Cause of Delay	Impact / Risk	Correction Needed
Alert acknowledged					<input type="checkbox"/> Yes <input type="checkbox"/> No
HR notification					<input type="checkbox"/> Yes <input type="checkbox"/> No
Legal counsel notification					<input type="checkbox"/> Yes <input type="checkbox"/> No
IT preservation started					<input type="checkbox"/> Yes <input type="checkbox"/> No
Device secured					<input type="checkbox"/> Yes <input type="checkbox"/> No
Employee access restricted					<input type="checkbox"/> Yes <input type="checkbox"/> No
JPA/insurer notice review					<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
External reporting review					<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

5. Policy and Procedure Clarity Review

Use this section to identify whether staff knew which policy, protocol, form, contact list, or approval path applied during the response.

Policy / Procedure Area	Clear?	Unclear or Missing Issue	Recommended Update Owner	Target Date
Alert routing / designated response lead	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial			
Evidence preservation / chain of custody	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial			
Employee access restriction	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial			
Administrative leave coordination	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			
Mandated reporting review	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial			
JPA/insurance notice	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			
Board / parent / media communication approval	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			

6. Evidence Preservation Review

Review whether evidence, records, logs, devices, and accounts were preserved properly and whether any handling created avoidable risk.

Preservation Area	Preserved?	Timing	Issues / Exceptions	Follow-Up Needed
Device secured from further use	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A			
Alert record preserved	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A			
Chain-of-custody log started	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A			
Authentication / network logs preserved	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A			
Email / cloud records preserved	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A			
Suspicious content not accessed/copied/sent	<input type="checkbox"/> Confirmed <input type="checkbox"/> Unable to confirm			

Preservation Area	Preserved?	Timing	Issues / Exceptions	Follow-Up Needed
Forensic or law enforcement handling considered	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A			

7. Access Containment Review

Review whether access was restricted quickly and appropriately based on district direction, HR coordination, legal review, and student-safety considerations.

Access Area	Reviewed?	Restricted / Disabled?	Timing	Issue / Gap
Laptop / district device	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
Email	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
Cloud storage / shared drives	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
SIS / LMS	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
VPN / remote access	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
Building badge / physical access	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
District phone / messaging tools	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		
Administrative systems	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A		

8. Communication Control Review

Review whether communications were limited, accurate, timely, and routed through the appropriate approval process.

Communication Area	Controlled?	Reviewed / Approved By	Issues / Gaps	Recommended Fix
Internal response team communications	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial			
Board notification	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			
Parent/guardian communication	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			
Staff communication	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			
Media / public statement	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			
JPA / insurer communication	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Partial <input type="checkbox"/> N/A			

9. Training Gaps

Identify training needs discovered during the incident response. Training gaps may involve awareness, escalation, documentation, preservation, communications, or role clarity.

Training Area	Gap Identified?	Who Needs Training?	Recommended Training / Action	Priority
Digital risk alert routing	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
Evidence preservation basics	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
Chain-of-custody documentation	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
Mandated reporting awareness	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low

Training Area	Gap Identified?	Who Needs Training?	Recommended Training / Action	Priority
Employee access restriction process	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
Board/parent/media communication control	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
Tabletop exercise readiness	<input type="checkbox"/> Yes <input type="checkbox"/> No			<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low

10. Recommended Policy / Procedure Updates

List recommended changes to policies, procedures, contact lists, forms, training materials, or vendor/JPA coordination workflows.

Recommended Update	Reason / Issue Addressed	Owner	Target Date	Status
				<input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Complete
				<input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Complete
				<input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Complete
				<input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Complete
				<input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Complete
				<input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Complete

11. Corrective Action Summary

Question	Response
What were the three most important things that worked well?	1. 2. 3.
What were the three most important things that need improvement?	1. 2. 3.
What immediate corrective action should be completed within 30 days?	
What longer-term corrective action should be completed within 90 days?	
Is another tabletop exercise recommended?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> To be determined
Who owns follow-up tracking?	

12. Review Completion and Sign-Off

Field	Response
Review completed by	
Title / role	
Date completed	
Legal counsel review needed?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Already completed
JPA/risk pool follow-up needed?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Already completed <input type="checkbox"/> N/A
Policy/procedure update owner	
Next review date, if applicable	

13. Review Reminder

A post-incident review should strengthen the next response, not relitigate every decision made under pressure.

Capture what worked. Identify what was delayed. Fix unclear procedures. Train the right people. Improve the process before the next alert.

Disclaimer and Use of Materials

The NetPropriate Digital Risk Response Packet and related response guides, forms, logs, worksheets, 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.