NetPropriate®
DISCOVER HIDDEN DIGITAL RISK | FIND PREDATORY BEHAVIOR

Evidence Preservation Response Guide

What Not to Touch, What to Preserve, and How to Protect Chain of Custody

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 first response can significantly affect the integrity of any later administrative review, HR process, legal analysis, law enforcement referral, forensic examination, insurance claim, or civil proceeding.

This guide is intended to help districts, JPAs, legal counsel, HR teams, administrators, IT personnel, and other authorized response personnel understand basic evidence-preservation principles after a digital risk alert.

The goal is not to conduct a full forensic investigation internally. The goal is to prevent unnecessary handling, preserve relevant records, maintain a clear chain of custody, and allow the appropriate legal, forensic, administrative, or law enforcement process to proceed without avoidable contamination.

Evidence Preservation Scope Note

This guide is provided for general preservation-awareness and planning purposes only. NetPropriate does not provide forensic advice, legal advice, law enforcement direction, mandated reporting instruction, evidence-handling certification, or investigative direction. NetPropriate does not determine whether content is criminal, whether evidence is admissible, whether a device should be imaged, whether law enforcement should seize a device, or whether a specific report must be made. All decisions involving evidence handling, forensic imaging, chain of custody, law enforcement contact, mandated reporting, employee discipline, student safety, legal holds, insurance/JPA notice, or external reporting should be made by the appropriate district officials in coordination with legal counsel, qualified forensic professionals, JPAs/risk pools, insurers, mandated reporters, law enforcement, child protective agencies, or other authorized entities.

2. Evidence Preservation Guiding Principle

After a digital risk alert, the safest first response is usually:

Stop. Preserve. Limit access. Document. Escalate.

Personnel should avoid curiosity-driven review. Opening files, forwarding screenshots, copying suspected material, deleting files, moving folders, or allowing the assigned user to continue using the device may create unnecessary risk.

The district's first preservation objective is to maintain the condition of the device, account, alert data, and related records as close as possible to the state in which they existed when the alert was identified.

3. Immediate Preservation Priorities

Upon receiving a NetPropriate alert or other digital risk notice, the district should promptly identify and preserve relevant information.

Immediate preservation priorities may include:

- The district-managed device;
- The assigned user account;
- The NetPropriate alert record;
- File path, hash-match, or alert metadata;
- Device serial number and asset tag;
- Device assignment history;
- Login and authentication records;
- Network access logs;
- Web-filtering logs, if applicable;
- Email and cloud-storage records;
- Local user profile information;
- Backup or snapshot records;
- Acceptable Use Policy acknowledgments;
- Prior technology-use reports or complaints;
- HR/personnel records, where relevant;
- Chain-of-custody documentation.

4. What Personnel Should Not Do

Well-intentioned internal review can unintentionally compromise evidence or create additional legal exposure.

Personnel should not:

- Open suspicious files to “see what they are”;
- Preview images or videos out of curiosity;
- Copy files to a thumb drive, desktop folder, cloud location, or email;
- Forward screenshots, filenames, images, videos, or file samples;
- Delete, quarantine, rename, move, or alter suspicious files;
- Ask IT to search broadly without counsel-directed parameters;
- Continue using the device for normal work;
- Allow the assigned user to retain access to the device or account if containment is warranted;
- Run cleanup tools, antivirus remediation, or system updates without direction;
- Restart, wipe, reimage, reset, or redeploy the device unless directed;
- Change passwords or terminate sessions without considering preservation impact;
- Discuss alert details with staff who do not have a need to know;
- Document conclusions before the facts are reviewed by appropriate authorities.

The objective is to preserve the evidence, not to prove the alert through informal internal review.

5. Device Preservation

When a device is associated with an alert, the district should preserve the device and prevent unnecessary use.

Device preservation may include:

- Identifying the physical device;
- Recording the device type, make, model, serial number, and asset tag;
- Identifying the assigned user;
- Recording the date and time the device was located;
- Photographing the exterior condition of the device, if appropriate;
- Documenting whether the device was powered on, asleep, locked, connected to power, or connected to a network;
- Limiting access to authorized personnel;
- Securing the device in a locked location;

- Waiting for counsel, law enforcement, or forensic direction before imaging, powering down, disconnecting, or manipulating the device.

Whether to leave a device powered on, power it down, disconnect it from the network, or capture volatile memory can be fact-specific. Those decisions should be made with legal counsel, qualified forensic personnel, or law enforcement when appropriate.

6. Account and Cloud Preservation

Digital evidence may not live only on the physical device. Relevant information may also exist in cloud systems, email platforms, browser sync, shared drives, learning platforms, identity systems, security tools, or backup environments.

The district should consider preserving:

- Email accounts;
- Cloud storage accounts;
- Browser sync data;
- File-sharing records;
- Learning management system access;
- Student information system access logs;
- Authentication/MFA logs;
- VPN logs;
- Web-filtering records;
- Endpoint security logs;
- Backup or retention snapshots;
- Admin audit logs;
- Shared drive permissions;
- Account assignment and access history.

Account restrictions should be coordinated carefully. For example, disabling an account may be appropriate for containment, but the district should consider whether doing so affects logs, sessions, retention settings, or cloud evidence.

Legal counsel and IT should coordinate before account changes are made.

7. Log Preservation

Logs can be highly time-sensitive. Some systems overwrite, rotate, or age out logs after a short retention period.

The district should identify which logs may be relevant and preserve them promptly.

Potential logs may include:

- Device login logs;
- Network authentication logs;
- VPN logs;
- Web-filtering logs;
- Firewall logs;
- Endpoint detection logs;
- Email audit logs;
- Cloud storage access logs;
- File creation, modification, or access timestamps;
- Browser history or sync records, where available and legally appropriate;
- Identity provider logs;
- MFA logs;
- Print logs;

- Remote-access logs;
- Administrative action logs.

The district should document who preserved the logs, when they were preserved, where they were stored, and whether the preserved copy is complete.

8. Chain of Custody

Chain of custody is the documented history of who had possession or control of evidence, when they had it, why they had it, and what happened to it.

For digital risk alerts, chain-of-custody documentation should begin as soon as the device, account, alert, or related record is preserved.

A chain-of-custody log should include:

- Date;
- Time;
- Item or evidence description;
- Device serial number, asset tag, account name, or record identifier;
- Location found;
- Condition when found;
- Person releasing the item or record;
- Person receiving the item or record;
- Reason for transfer;
- Storage location;
- Access restrictions;
- Notes regarding any handling, copying, imaging, or review;
- Signature or acknowledgment, where appropriate.

If an item changes hands, the log should be updated every time.

9. Alert Record Preservation

The NetPropriate alert itself should be preserved as part of the district's response record.

The preserved alert record may include:

- Alert date and time;
- Recipient of the alert;
- User or device associated with the alert;
- Device identifier;
- File path or location information, where available;
- Hash-match information, where available;
- Alert category or severity;
- Any automated system metadata;
- District response actions;
- Personnel notified;
- Preservation steps taken;
- Follow-up actions assigned.

The alert record should be preserved without expanding unnecessary access to suspected content.

If the alert involves hash-matched or otherwise flagged material, personnel should avoid attempting to independently open or verify the underlying content unless directed by counsel, law enforcement, or a qualified forensic examiner.

10. Suspected CSAM or Child Exploitation Concerns

If an alert may involve suspected child sexual abuse material, child exploitation, online enticement, child sex trafficking, or unlawful sexual content involving minors, the district should treat the matter as high severity.

Personnel should not open, copy, forward, screenshot, transmit, or distribute suspected material.

The appropriate response may include immediate coordination with:

- District legal counsel;
- Mandated reporters;
- Law enforcement;
- Child protective agencies;
- NCMEC CyberTipline;
- Qualified forensic professionals;
- JPA/risk pool or insurer, where applicable.

11. Role Clarity During Preservation

Evidence preservation requires clear lanes.

IT's role

IT may assist with:

- Identifying devices;
- Restricting access;
- Preserving logs;
- Maintaining asset records;
- Exporting system metadata;
- Supporting forensic preservation;
- Documenting technical steps taken.

IT should not be asked to conduct an informal criminal investigation or independently determine whether content is unlawful.

HR's role

HR may assist with:

- Employee access restrictions;
- Administrative leave coordination;
- Personnel record preservation;
- Policy acknowledgment records;
- Employee communication;
- Union or representation coordination.

HR should avoid characterizing the evidence or drawing conclusions before appropriate review.

Administration's role

Administrators may assist with:

- Student safety containment;
- Site operations;
- Internal coordination;
- Board awareness;
- Communications discipline;
- Ensuring the right personnel are involved.

Administrators should avoid broad disclosure or informal witness questioning.

Legal counsel's role

Legal counsel may assist with:

- Preservation instructions;
- Privilege protocols;
- Reporting analysis;
- Law enforcement coordination;
- Forensic examiner engagement;
- HR and employment coordination;
- JPA/insurance notice;
- Communications review.

12. Forensic Imaging and Examination

Forensic imaging or deeper examination should generally be handled by qualified forensic personnel or law enforcement when appropriate.

The district should not assume that ordinary IT copying, drag-and-drop duplication, screenshots, or manual file review will preserve evidence properly.

Depending on the circumstances, counsel or law enforcement may determine whether to:

- Preserve the device without further action;
- Create a forensic image;
- Capture volatile memory;
- Preserve cloud records;
- Export logs;
- Use an outside forensic examiner;
- Transfer the device to law enforcement;
- Maintain the device in district custody pending direction.

These decisions are fact-specific and should be documented.

13. Communications About Evidence

Personnel should avoid unnecessary written commentary about suspected evidence.

Written communications should be factual, limited, and process-focused.

Preferred wording:

> "A digital risk alert was received involving a district-managed device. The device, alert record, and related access information are being preserved pending further direction from district leadership and counsel."

Avoid wording such as:

> "We found illegal material on the employee's laptop."

Unless an authorized determination has been made, records should avoid legal conclusions, inflammatory descriptions, speculation, or assumptions about intent.

Personnel should also avoid sending detailed descriptions of suspected content to broad email groups, board members, staff, or anyone without a defined response role.

14. Storage and Access Control

Preserved devices and records should be stored securely.

Storage and access-control practices may include:

- Locked physical storage;

- Limited key or badge access;
- Restricted digital folders;
- Access logs;
- No shared passwords;
- No informal copying;
- No personal cloud storage;
- No use of personal devices;
- No forwarding to private email accounts;
- No removal from district custody without documentation;
- Separate privileged or counsel-directed folders where appropriate.

Only authorized personnel should access preserved evidence, and each access should be documented when the evidence itself is touched, transferred, copied, imaged, or reviewed.

15. Preservation Timeline

A simple preservation timeline should be maintained from the first alert forward.

The timeline should include:

- When the alert was received;
- Who received it;
- Who was notified;
- When the device was located;
- Who had possession of the device;
- Whether the device was powered on, locked, connected, or in use;
- When account access was restricted;
- When logs were preserved;
- When counsel was contacted;
- When HR was contacted;
- When JPA/insurer notice was considered or completed;
- When law enforcement, CPS, NCMEC, CTC, or other agencies were contacted, if applicable;
- When any forensic examiner was engaged;
- When any transfer, imaging, review, or storage action occurred.

The timeline should be factual and should avoid speculation.

16. Common Evidence Preservation Mistakes

Districts should train personnel to avoid common mistakes, including:

- Treating the alert as a routine helpdesk issue;
- Allowing multiple people to inspect the device;
- Opening files to confirm the alert;
- Forwarding screenshots or suspected files;
- Deleting or quarantining material without direction;
- Continuing to use the device;
- Reassigning or reimaging the device too quickly;
- Failing to preserve cloud records or logs;
- Forgetting to document chain of custody;
- Allowing the assigned user to retain access when containment is warranted;
- Discussing suspected content broadly;
- Failing to involve counsel early;
- Waiting too long to preserve logs;
- Using imprecise or inflammatory language in emails.

The safest approach is to preserve first and investigate only through the proper channel.

17. Evidence Preservation Checklist

Immediate Evidence Preservation Checklist

- Confirm receipt of the alert.
- Identify the device, account, user, and location.
- Preserve the alert record and metadata.
- Do not open, copy, forward, delete, move, rename, or alter suspicious content.
- Secure the device and prevent further use.
- Record the device serial number, asset tag, condition, and assigned user.
- Document whether the device is powered on, asleep, locked, connected, or offline.
- Notify legal counsel and designated district leadership.
- Coordinate with HR regarding employee access and device recovery.
- Preserve relevant account, cloud, authentication, network, and web-filtering logs.
- Restrict access to preserved records.
- Begin a chain-of-custody log.
- Document every transfer, access event, preservation step, and decision.
- Determine whether forensic imaging or law enforcement handling is needed.
- Evaluate whether mandated reporting, NCMEC, CPS, CTC, JPA, insurer, or other notice may be implicated.
- Avoid broad internal communication or speculative written conclusions.

18. Evidence Preservation Guiding Principle

Evidence preservation is not about doing more.

It is about preventing the wrong thing from being done too soon.

> **Do not touch what does not need to be touched. Preserve what may matter. Document who handled it. Escalate to the right authority. Keep the record clean.**

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.