Administrative Procedure 7234

DIGITAL FORENSICS AND INVESTIGATIONS PROCEDURE

Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure establishes the requirements and processes for the authorization, collection, preservation, analysis, and handling of digital evidence during District-authorized investigations involving District information systems, accounts, or devices.

The purpose of this procedure is to:

1. Support District disciplinary, administrative, and information security investigations;
2. Preserve the integrity, reliability, and availability of digital evidence;
3. Protect the privacy rights of students, employees, and other users consistent with District policy and applicable law; and,
4. Ensure investigations are conducted in a consistent, expedient, defensible, and minimally intrusive manner.

DEFINITIONS

1. "Chain of Custody" refers to documentation demonstrating the control, transfer, analysis, and disposition of evidence.
2. "Digital Evidence" refers to data of potential investigative value that is stored or transmitted in digital form.
3. "eCompliance Group" refers to the District's group responsible for approving or rejecting access to District content, audit log review, or eDiscovery search of any District account as determined by Admin Regulation 7206 – "eDiscovery – Data Compliance, Search, and Investigation"
4. "Forensic Collection" refers to the process of identifying, collecting, acquiring, and preserving digital evidence.
5. "Investigation Authorizing Authority" or "Authorizing Authority" refers to the designated individual, role, or governing body with the formal power to approve, initiate, or mandate an investigation. The Authorizing Authority does not conduct the investigation directly; rather, they validate the need and scope of the investigation, allocate resources as applicable, and provide the official authorization required for the investigation to occur.

6. "Investigation Requestor" or "Requestor" refers to the individual or authorized party who initiates a formal request for an investigation due to an alleged incident, concern, or policy violation.
7. "Remote Collection" refers to evidence collection performed without physical possession of a device.
8. "Scope" refers to the defined boundaries of an investigation, including timeframe, systems, accounts, and behaviors under review.

PROCEDURE

1. Roles and Responsibilities
    a. Authorizing Authority
        i. Authorizes digital forensic investigations based on legal, regulatory, personnel, or academic needs.
        ii. Requests eDiscovery approval through the eCompliance group as necessary.
        iii. The Authorizing Authority may differ based on the scope, subject, and requirements of the investigation, but is limited to the following:
            1. School Administration – authorizes student conduct related investigations.
            2. General Counsel – authorizes investigations related to District regulations, compliance, and litigation (legal hold).
            3. Human Resources, Department of Labor Relations – authorizes investigations related to employee misconduct including potential violations of WCSD Policy, Regulation, and Procedure.
            4. School Police – authorizes investigations related to criminal activity. The School Police department acts as a proxy to external law enforcement agencies and may receive requests to preserve evidence when cases are referred to them.
            5. IT Security Officer – authorizes digital forensics related to IT Security incidents that may cause imminent harm to the Confidentiality, Integrity, or Availability of District Information Resources.

b. Investigation Requestor

    i. Seeks approval through the appropriate School or Department Authorizing Authority to perform an investigation.

    ii. Coordinates with the IT Security Department to provide the appropriate scope, parameters, and timing of the investigation upon documented approval from the designated Administrator and Investigation Approving Authority.

c. School or Department Approving Authority

    i. Serves as the senior authority in a School or Department.

    ii. Validates an Investigation Requestor's need and scope for an investigation due to alleged or actual misconduct.

    iii. Seeks approval through the appropriate authorizing authority to perform an investigation.

    iv. Coordinates with the IT Security Department to provide the appropriate scope, parameters, and timing of the investigation.

d. Office of Information Technology

    i. Chief Information Officer.

    ii. Oversees Digital Forensics and Investigations by allocating personnel, technical, and financial resources to support District digital forensics and investigatory requirements.

    iii. IT Operations and Services Departments.

    iv. Provides technical assistance and operational support to the IT Security Department under the direction of the Chief Information Officer.

    v. IT Security Department.

    vi. Performs digital forensic investigations, including evidence collection, analysis, tracking, documentation, and reporting in support of District requirements.

2. Authorization and Approval

    a. The District provides information systems and digital resources for legitimate educational and business purposes. Digital forensic activities

may be conducted to support District disciplinary, administrative, or information security investigations.

b. While users of District information systems have no expectation of privacy when using District-owned or District-managed systems, accounts, or networks, all digital forensic investigations require explicit authorization from the appropriate authority prior to evidence collection.

c. Digital forensic investigations may be conducted when authorized by the appropriate School or Department Administrator, the appropriate Authorizing Authorities, and the District's eCompliance group as applicable and under the following circumstances:

    i. Suspected violations of District policies, procedures, or acceptable use requirements;

    ii. Employee misconduct or administrative investigations supported by Human Resources, Legal, or Labor Relations;

    iii. Student-related investigations involving misuse of District systems, accounts, or devices;

    iv. Information security incidents, including suspected malware, unauthorized access, data exposure, or abuse of access;

    v. Requests to support compliance with legal, regulatory, or records retention obligations;

    vi. Other circumstances deemed necessary by the District to protect the confidentiality, integrity, or availability of District information systems.

d. For investigations involving litigation, public records requests, or legal hold obligations, forensic activities shall be coordinated with Legal Services to ensure compliance with applicable eDiscovery and records retention requirements.

e. If suspected criminal activity is identified during a District investigation, IT Security shall preserve existing evidence, cease investigative expansion, and notify the appropriate authority.

3. Investigation Scope and Parameters

    a. A documented investigative scope shall define the approved parameters of the investigation, including timeframes, systems, accounts, and/or behaviors under review.

b. The Investigation Requestor shall document the scope and request approval from the appropriate School or Department Administrator and the Investigation Approving Authority.

c. Authorization for forensic investigations shall define, at a minimum:

    i. The reason for the investigation;

    ii. The systems, accounts, or devices involved;

    iii. The behaviors or concerns under review; and

    iv. The approved timeframe for evidence collection and analysis.

    v. The scope shall be established and approved prior to evidence collection.

d. The Requestor shall coordinate with the IT Security Department to provide relevant information necessary to complete the investigation and to the investigative needs, requirements, and authorized scope of the investigation.

    i. The IT Security Department shall not expand investigative scope beyond the authorized parameters without documented approval from the requestor and authorizing authority.

    ii. If, during the course of a limited-scope analysis, evidence of severe misconduct or potential criminal activity outside the authorized scope is discovered, IT Security shall document the observation, cease further analysis of the unrelated material, and seek expanded authorization or refer the matter to the District School Police Department or appropriate law enforcement agency, as directed by the authorizing authority.

4. Evidence Collection

a. Digital evidence may be identified and collected using methods appropriate to the circumstances, including remote or logical collection, log or artifact collection, or physical acquisition of devices.

b. Evidence collection activities shall be conducted in a manner that:

    i. Preserves the integrity of data;

    ii. Minimizes disruption to District operations; and,

    iii. Avoids unnecessary alteration of data.

c. Upon receipt of physical or acquisition of logical evidence, the IT Security Department shall make two (2) forensically sound exact copies of the evidence.

d. Analysis performed shall be against a duplicated copy of the original evidence.

5. Evidence Tracking and Documentation

a. Evidence documentation shall be created and maintained to ensure proper handling, safeguarding, and tracking of evidence. Ensuring that evidence is controlled and accounted for throughout all phases of the investigation, is critical to the integrity of the District's investigative process and the defensibility of investigation outcomes.

b. Evidence documentation shall include, where applicable, dates and times of acquisition, Chain of Custody records, and Asset identifiers (serial numbers, system characteristics, and operating system information).

c. Physical devices collected as evidence shall be documented using the District's "Evidence Chain-Of-Custody Tracking Form" or an equivalent Chain of Custody record reflecting:

i. Submitting employee:

1. The name, unique identifier (typically EmployeeID), and contact information of the person who collected the evidence;

2. The date/time seized;

3. Any associated IT Ticket numbers; and,

4. Location seized.

ii. Description of the Evidence:

1. Chain of Custody item number;

2. Quantity;

3. Description of the item (model, serial #, condition, distinguishing marks or other physical characteristics); and,

4. Tamper seal serial numbers (if applicable).

iii. Chain of Custody

1. Chain of Custody item number;
2. Date/time an activity occurred;
3. Person transferring evidence from;
4. Recipient;
5. Comments; and,
6. Location of event.

iv. Disposition:

1. Disposal determination (destruction or release to owner);
2. Witness to destruction of evidence; and/or,
3. Confirmation of release to owner.

d. Evidence collected through remote or logical means shall be documented through evidence logging and logical integrity checks (cryptographic signature) by IT Security personnel performing the collection. Documentation shall include the collection method, date and time of collection, systems involved, and responsible personnel.

e. Evidence records shall be updated anytime an investigator handles or works on the original evidence after it has been collected.

6. Analysis and Reporting

a. Analysis of digital evidence shall be limited to the authorized investigative scope and conducted using tools and techniques approved by the IT Security Department.

b. Investigative findings shall be documented objectively and communicated to the authorizing authority as appropriate to the case.

c. Estimated timelines for evidence collection, analysis, and review may be provided upon request; however, timelines are dependent on investigative scope, complexity, and resource availability.

7. Case Closure and Escalation

a. Upon completion of an investigation, the disposition of devices and digital evidence shall be determined by the Authorizing Authority.

b. Digital evidence shall be confidential, secured, access-controlled, and retained in accordance with District retention requirements.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:

    a. Administrative Regulation 7211 "Responsible Use and Internet Safety";

    b. Administrative Procedure 7208 "IT Cybersecurity"; and

    c. Applicable local, state, and federal laws and regulations.

REVISION HISTORY

Date	Revision	Modification
03/19/2026	1.0	Adopted