Administrative Regulation 7206
eDISCOVERY – DATA COMPLIANCE, SEARCH, AND INVESTIGATION

Responsible Office: Office of Information Technology

PURPOSE

This Administrative Regulation describes the process by which eDiscovery requests are handled related to electronic searches and investigations, and how access is granted to individuals in the Washoe County School District (District) when requested.

DEFINITIONS

1. "Audit Log Search" refers to the ability to search all logs within Microsoft Office 365 for data.
2. "Case" refers to the container created to hold all of the discovered data.
3. "Content search" refers to the ability to search all electronic data within the District network.
4. "Data" refers to any and all forms of electronic communication and storage that use the District network for transmission or storage.
5. "Documents" refers to any documents, pictures, or files of any kind, and having any valid file extension which are stored in Office 365 using OneDrive, SharePoint and/or Microsoft Teams document storage.
6. "eDiscovery" refers to the process of searching all electronic communications within the District for specific data upon request of the Office of the General Counsel, to include a litigation hold request.
7. "Email" refers to electronic messaging over a communications network.
8. "Litigation hold" (also known as "preservation orders" or "hold orders") refers to a stipulation requiring the District to preserve all data that may relate to a legal action involving the District. This requirement ensures that the data in question will be available for the discovery process prior to or during litigation.
9. "Retention Period" refers to the amount of time that the District will maintain user data after departure from the District for any reason. The length of time the District retains data is dependent on the job title and role the person had within the District and complies with the current version of the Nevada Local Government Records Retention Schedules.

REGULATION

1. Data Privacy Expectations / Responsibilities

    a. Employees, students, and others using the District network have no guarantee or unfettered right of privacy when using the District network and any of the tools associated with it, such as email and document storage, whether personal or shared.

    b. Anything created and or stored on the District's network is the property of the District and may be subject to release under a public records request, and/or to search, and/or to eDiscovery in the event of an investigation or lawsuit.

    c. The Office of Information Technology, on occasion, may access, review, move, or delete items for the health of the network so long as those deletions are not in violation of the Nevada Local Government Records Retention Schedules or a litigation hold.

    d. The District has the right to:

        i. monitor, review, and inspect all electronic storage and communications including emails, files, video teleconferences, and any other digital data; and

        ii. disclose all data created, saved, or accessed under any user account when required by, or permitted by law.

    e. District data and file storage locations must be approved by the Office of Information Technology. The primary authorized storage locations are the washoeschools.net and washoeschools.org Office 365 domains. Other file storage providers may be explicitly authorized for limited use.

        i. At no time should any District user copy, create, or move any District data to unauthorized third-party storage providers including, but not limited to, personal Google Drive, Yahoo, Go Daddy, Dropbox, and Box accounts.

        ii. Users must not transfer District data to personal electronic storage including but not limited to external hard drives, flash drives, optical discs (CD, DVD, Blu-rays, etc.), and other removable media.

    f. Student created work and documents may be stored in approved storage locations and Digital Learning Tools (DLTs). Students should use OneDrive in Office 365 for any persistent data storage due to infrastructure protections, eDiscovery capabilities, and compliance restrictions.

2. Retention

    a. The Office of Information Technology has established a data retention schedule for all data within the District network and complies with the current version of the Nevada Local Government Records Retention Schedules for retention of electronic information.

3. Access Requests Requiring eCompliance Group Approval

    a. The eCompliance Group is comprised of:

        i. Chief Information Officer, or designee;

        ii. Information Technology Security Officer, or designee;

        iii. Chief General Counsel, or designee;

        iv. Chief of Human Resources, or designee; and

        v. Chief of School Police, or designee.

    b. Except as otherwise provided in this Administrative Regulation, before any Content, Audit Log, or eDiscovery search of any account is conducted, every member of the eCompliance Group must approve the request.

    c. Access to Current or Former Employee and Student Accounts

        i. Requests to access the account of a current or former District employee or student shall be emailed to the eCompliance Group. Requests must be handled through email in all cases, EXCEPT when the person under investigation is part of, or has a link to the eCompliance Group which would make it impossible to send an email request without alerting the individual(s) under investigation. The email request MUST include the following:

            1) What information is being sought and whose account(s) should be searched.

            2) Why access is requested, e.g., authorized investigation (excluding investigations by the Office of the General Counsel Administrative Investigations Division), administrative discipline, etc.

        ii. In the event a member of the eCompliance Group is the person under investigation, is involved in the investigation, or an email would alert the individual(s) being investigated, the requester shall walk the request through the remaining members of the

eCompliance Group for signature and approval before the search will be allowed.

iii. If the request is approved by the eCompliance Group, the Office of Information Technology shall conduct a search matching the parameters in the request and provide the requester with the search results.

iv. Searches of the Account of the Superintendent

1) In a case where the Superintendent is the subject of a search or investigation, the request and authorization for access to his/her account must come from the President of the Board of Trustees (Board) to the Chief Information Officer. An email or letter from the Board President will be required to initiate the search and will serve as proof of approval.

v. If the Superintendent requests access to an account, he/she must notify the Board President of his/her intentions. A copy of the Superintendent's email or letter to the Board President will serve as proof of notification. The Superintendent shall follow the same process of notifying the eCompliance Group of the search.

1) The members of the eCompliance Group may deny the request and give reasoning behind his/her denial. A denial will not override the Superintendent's request for access, but it will allow for documentation of any concerns from the group.

4. Access Requests Exempt from eCompliance Group Approval

a. Public Records Requests

i. Pursuant to Board Policy 7610 – Public Records Requests, the Office of the General Counsel receives and processes public records requests under Nevada's Public Records Act (NPRA).

ii. Upon receipt of a public records request, the Office of the General Counsel may conduct an eDiscovery and/or content search to comply with the request and NPRA. A notation shall be made by the Office of the General Counsel on the eDiscovery search indicating it was conducted to comply with NPRA.

iii. These requests are exempt from requesting eCompliance Group approval.

b. Investigations by the Office of the General Counsel Administrative Investigative Division

    i. At the direction of the Superintendent and pursuant to Administrative Regulation 9166 – Administrative Investigations, the Administrative Investigations Division of the Office of the General Counsel provides internal investigative support for District representatives, including the Board, the Superintendent and Administrators of the District.

    ii. Upon receipt of a public records request, the Office of the General Counsel Administrative Investigator may conduct an eDiscovery and/or content search. A notation shall be made by the Office of the General Counsel Administrative Investigator on the eDiscovery search indicating it was conducted as part of an authorized administrative investigation.

    iii. These requests are exempt from requesting eCompliance Group approval.

c. Searches by the Office of the General Counsel for Legal Purposes

    i. At the direction of the Superintendent and pursuant to Administrative Regulation 9165 – Legal Counsel, the Office of the General Counsel provides legal services to District representatives, including the Board, the Superintendent and Administrators of the District. In order to provide these services, eDiscovery content searches may be necessary.

    ii. The Office of the General Counsel may conduct an eDiscovery and/or content search at the direction of the Chief General Counsel, Deputy Chief General Counsel or General Counsel. A notation shall be made on the eDiscovery search indicating at whose direction the search was conducted.

    iii. These requests are exempt from requesting eCompliance Group approval.

d. Standard Information Technology work order

    i. In order to allow employees to perform their normal day-to-day duties, regular requests to retrieve deleted email, missing email, or perform other maintenance and repair on an individual's account are exempt from notifying the eCompliance distribution group, or from seeking authorization from that group. Whenever Information Technology receives a request for this type of search, Information Technology will generate a work order to ensure compliance, and

as a check and balance against unregulated and/or unauthorized searches.

ii. The name of the person requesting this search must match the name of the account to be searched.

e. Information Security Threats – exempt from eCompliance Approval:

i. In order to allow the organization to respond to emerging Information Technology Security threats, designated employees perform regular search and destroy activities against organizational information systems. Quick reaction to Information Technology Security threats minimizes the risk of loss to the District. Searches that find and delete malicious content are exempt from notifying the eCompliance distribution group, or from seeking authorization from that group.

ii. Information Security Threat activities will be audited and consolidated in regular eDiscovery reporting.

5. Frequency and distribution of eDiscovery report

a. Upon request by the eCompliance Group and the Superintendent, the Office of Information Technology will produce and distribute a report documenting all eDiscovery, public records requests, and Information Technology work orders that generated a search. The report will confirm that no searches were conducted without prior notice and/or authorization.

b. All recorded searches included in this report must match up with an Information Technology work order, a public records request search notification email, or an eDiscovery approval email. Searches that appear in the report that do not have the appropriate accompanying documentation will be subject to investigation by the Office of Information Technology, Office of the General Counsel, and potentially the Superintendent and/or their designee, and could result in disciplinary action.

6. The "Roles" defined in the Permissions/Security and Compliance section of Office 365 are as follows:

a. Compliance Administrator

i. Description: Manage settings for device management, data loss prevention, reports, and preservation.

ii. Members: Chief Information Officer, Information Technology Security Officer, Designated Network Analysts, Security Analysts.

b. eDiscovery Manager

i. Description: Perform searches and place holds on mailboxes, SharePoint Online Sites, and OneDrive for Business Locations.

ii. Members: Chief Information Officer, Information Technology Security Officer, Chief General Counsel or designee, Designated Network Analysts, Security analysts.

c. Organization Management

i. Description: Control permissions for accessing features in the Security & Compliance Center, and manage settings for device management, data loss prevention, reports, and retention. NOTE: Office 365 automatically adds global admins as members of this group.

ii. Members: Chief Information Officer, Information Technology Security Officer, Designated Network Analyst, Security Analysts.

d. Reviewer

i. Description: Members can only view the list of cases on the eDiscovery cases page in the Security & Compliance Center. They cannot create, open, or manage an eDiscovery case. The primary purpose of this role group is to allow members to view and access case data in advanced eDiscovery.

ii. This role group has the most restrictive eDiscovery-related permissions.

e. Security Administrator

i. Description: Group membership is synchronized across services and managed centrally. This role group is not manageable through the administrator portals. Members of this role group may include cross-service administrators, as well as external partner groups and Microsoft Support. This group is not assigned roles by default. However, it will be a member of the Security Administrators role groups and will inherit the capabilities of that role group.

ii. All of the read-only permissions of the Security reader role, plus a number of additional administrative permissions for the same services: Identity Protection Center, Privileged Identity Management,

Monitor Office 365 Service Health, and Office 365 Security & Compliance Center.

iii. Members: Information Technology Security Officer.

f. Security Reader

i. Description: Members have read-only access to a number of security features of Identity Protection Center, Privileged Identity Management, Monitor Office 365 Service Health, and Office 365 Security & Compliance Center.

ii. Members: As needed by applications.

g. Service Assurance User

i. Description: Access the Service Assurance section in the Security & Compliance Center. Members of this role group can use this section to review documents related to security, privacy, and compliance in Office 365 to perform risk and assurance reviews for their own organization.

ii. Members: Information Technology Security Officer, Security Analysts.

h. Supervisory Review

i. Description: Members can create and manage the policies that define which communications are subject to review in an organization.

ii. Members: Information Technology Security Officer, Security Analysts.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Regulation aligns and complies with the governing documents of the District, to include:

   a. Board Policy 7205, Information Technology – Data Access Policy;

   b. Board Policy 7210, Information Technology Services and Operations;

   c. Board Policy 7610, Public Records Requests; and

   d. Board Policy 7620, Records Management.

2. This Administrative Regulation aligns and complies with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC), to include:

a. NRS Chapter 239, Public Records.

REVISION HISTORY

Date	Revision	Modification
05/16/2022	1.0	Adopted