Administrative Procedure 7233

E-DISCOVERY - 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 when requested, in the Washoe County School District ("District" or "WCSD").

REGULATION

1. Data Privacy Expectations / Responsibilities

    a. Staff, students, and others using the WCSD network have no guarantee of privacy when using the WCSD 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, or e-discovery in the event of an investigation.

    c. The Information Technology Department on occasion may access, review, move, or delete items for the health of the network.

    d. The District has the right to:

        i. monitor, review, and inspect all emails, files, Skype conversations 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. The only authorized storage location for district data and file storage is the washoeschools.net and washoeschools.org Office 365 domain.

        i. At no time should any WCSD user copy, create, or move any WCSD data to a third party storage provider. This includes, but is not limited to, Google Drive personal accounts, Yahoo, Go Daddy, Drobox, and Box.

        ii. Student created work and documents may be stored in the WCSD GAFE (Google Apps for Education) domain. However, students should use OneDrive in Office 365 for any data storage due to e-

discovery capabilities and compliance restrictions when using anything other than the District's Office 365 environment.

2. Procedure

    a. The Information Technology Department has established a data retention policy for all data within the WCSD network. (See Appendix A)

    b. Every member of the E-compliance group (see below) or their designee must confirm and authorize Content Searches, Audit Log searches, or e-discovery requests. The only exception to this approval process is for a public records requests, as described below.

    c. Requests will be handled through email in all cases, EXCEPT when the person under investigation is part of, or has a link to the E-compliance group which would make it impossible to send out an email request without alerting the individual(s) under investigation.

    d. The email request MUST include the following:

        i. What you need access to (whose account(s))

        ii. Why you need the access – investigation, lawsuit, administrative discipline, etc.

        iii. Who the case manager will be that is conducting the search

    e. In the event a member of the E-compliance group is the person under investigation, is involved in the investigation, or an email would alert the individual(s) being investigated, the requestor shall walk the request through the remaining members of the E-compliance group for signature and approval before the search will be allowed.

3. Superintendent Only

    a. 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 to the Chief Information Officer. An email or letter from the Board of Trustees President will be required to initiate the search, and will serve as proof of approval.

    b. If the Superintendent needs to initiate a search, or requests access to an employee's account, the Superintendent must notify the President of the

Board of Trustees of his/her intentions. A copy of the email or letter to the President of the Board of Trustees will serve as proof of notification. The Superintendent shall follow the same process of notifying the E-Compliance group of the search unless a member of the E-Compliance group is the subject of the search. In that case, the notification will be hand delivered to members of the E-Compliance group.

c. The members of the E-Compliance group may deny the request and give reasoning behind their denial. A denial will not override the Superintendent request for access, but it will allow for documentation of any concerns from the group.

4. E-Compliance Group Membership.

   a. The members of the E-Compliance Group is as follows:

      i. Chief Information Officer, or designee

      ii. Information Technology Security Officer

      iii. Chief General Counsel, or designee

      iv. Chief of Human Resources, or designee

      v. Chief of School Police, or designee

      vi. Chief of Staff

   b. The “Roles” defined in the Permissions/Security and Compliance section of Office 365 are as follows:

      i. Compliance Administrator

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

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

      ii. E-Discovery Manager

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

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

iii. Organization Management

1. 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

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

iv. Reviewer

1. 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.

2. This role group has the most restrictive E-Discovery-related permissions.

v. Security Administrator

1. 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.

2. 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.

3. Members: Information Technology Security Officer

vi. Security Reader:

1. 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.

2. Members: As needed by applications

vii. Service Assurance User

1. 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.

2. Members: Information Technology Security Officer, Security Analysts

viii. Supervisory Review

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

2. Members: Information Technology Security Officer, Security Analysts

5. Types of E-Discovery and content search

a. Public Records Request -

i. The Office of the General Counsel shall receive and respond to public records requests under the Nevada Public Records Act or, when applicable, the Freedom of Information Act.

ii. Upon receipt of a public records request, a notification email shall be sent from the Office of the General Counsel to the E-Compliance distribution group stating the terms of the request and the purpose of the search.

1. This is for notification only and NOT for approval.

2. The Office of the General Counsel handles public records requests as part of their regular duties so this portion of the procedure is included to allow them to perform those duties in a timely fashion.

3. The notification email is for the protection of the person doing the search and the District overall and is meant as a check and balance against unregulated and/or unauthorized searches.

b. E-Discovery "on Hold" request

   i. The members of the E-Compliance group must approve the request.

   ii. The Information Technology Security Officer will open a new work order in Service Manager to document request.

   iii. E-Discovery case opened, use description of case and work order number for case name.

   iv. Place all accounts pertaining to the records request on hold.

   v. Run a search matching the parameters in the request.

   vi. Inform requester that search is complete and allow requester access to the search results.

   vii. Once requester is finished with search results close case.

   viii. Update and close work order in Service Manager.

c. Standard Information Technology work order – exempt from E-Compliance approval

   i. In order to allow staff 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 E-Compliance 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 we need to search.

iii. Open a new work order in Service Manager to document request. Name of person making request, and the search parameters.

iv. Create content search and create an export if requested.

v. Inform requester that search is complete and allow requester access to the search results.

vi. Once requester is finished with search results close case.

vii. Ticket in service manager updated and closed.

6. Frequency and distribution of E-Discovery report

   a. On a quarterly basis, the Information Technology Department will produce a report documenting all E-Discovery, public records requests, and Information Technology work orders that generated a search. The IT Department will distribute this report to all members of the E-compliance group and the Superintendent. This report is to confirm that there were no searches done on our email and document systems without prior notification and/or authorization. The Information Technology Department will generate and distribute this report on or about January 1, April 1, July 1, and October 1.

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

DEFINITIONS

1. Data refers to any and all forms of electronic communication and storage that uses the WCSD network for transmission or storage.

2. E-Discovery refers to the process of searching all electronic communications within the District for specific data upon request by the Office of the General Counsel, to include a litigation hold request.

3. Litigation hold refers to (also known as "preservation orders" or "hold orders") is 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 litigation.

4. Content search refers to the ability to search all electronic data within the WCSD network.

5. Audit Log Search refers to the ability to search all logs within the Microsoft Office 365 environment for data.

6. Email refers to the electronic messaging over communications network

7. Documents refers to the any documents, pictures, or files of any kind, and having any valid file extension which are stored in Office 365 using One Drive, SharePoint and/or Teams document storage

8. Skype refers to Information contained in all Skype for Business conversations

9. Case refers to the container created to hold all of the discovered data

10. Retention Period refers to the amount of time that the District will maintain user email and data after an employee leaves the district for any reason or after a student leaves 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 is included in Appendix A of this procedure.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This administrative procedures reflects the goals of the District's Strategic Plan and complies with the governing documents of the District, to include:

    a. Board Policy 7610, Public Information and Records Requests

    b. Board Policy 7620, Document and Records Management

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

    a. Chapter 239, Public Records

3. This document complies with federal laws and regulations, and specifically:

    a. Freedom of Information Act

REVIEW AND REPORTING

1. This procedure and any accompanying documents will be reviewed bi-annually in even numbered years.

REVISION HISTORY

Date	Revision	Modification
11/08/2017	1.0	Adopted

APPENDIX A

Type of Record / Document	Retention Period	Deleted Files / Email	Unrecoverable
Data Center – On Premise Servers	Commvault Backup – 50 days current de-duplicated data on-site Commvault Backup – 120 days de-duplicated data in Azure Cloud Commvault Backup – 2 Semi- Annually (January and July) non-de-duplicated data for 1 year	120 Days of Current Backups	1 year
Data Center – On Premise Storage	Azure Backup – Daily, Monthly, Yearly	1 year	1 year
Azure Servers	Azure Backup – Daily, Monthly, Yearly	1-year Azure Recovery Vaults size, limits on number of backups	1 year
School – On Premise Services	Azure Backup – Daily, Monthly, Yearly (Optional)	1 year	1 year
SharePoint (School and Department Sites)	18 Months after Account is Disabled	30 Days – Retrievable by User or IT 60 additional days - Retrievable by IT	Unlimited – E-Discovery
SharePoint (Groups and Teams)	18 Months after Account is Disabled	30 Days – Retrievable by User or IT 60 Additional Days – Retrievable by IT	90 Days following Deletion of Files – E-Discovery
One Drive (Staff and Student)	Staff - Retained for 4 years; Students – for 1 year	30 Days – Retrievable by User or IT 60 Additional Days – Retrievable by IT	90 Days following Deletion of Files – E-Discovery
End Point Devices (Desktop, Laptop, Tablets)	Data not retained	Data not retained	Unrecoverable
Email Storage	Staff - Retained for 4 years; Students – for 1 year	60 Days – Retrievable by User or IT	Staff - Retained for 4 years; Students – for 1 year
User Accounts	Staff - Retained for 4 years; Students – for 1 year		Staff - Retained for 4 years; Students – for 1 year