AURARIA HIGHER EDUCATION CENTER™

Policy Number 3.4.2

Chapter: Administration

Title: Records Management and Retention

Division/Department: Administration/Legal

Policy Administrator: General Counsel

Adoption Date: March 13, 1999

Revision Dates: May 15, 2024

1. PURPOSE

The purpose of this policy is to provide clarity, consistency, and guidance to the Auraria Higher Education Center (AHEC) for retention of Records, including Retention Periods, digitization, and disposition of such Records.

2. DEFINITIONS

2.1. AHEC Record (also referred to herein as "Record"): Any file, document, recorded sound, electronic message, email, or image made, maintained, or kept by AHEC, regardless of format (paper, digital, photographic, fiche, etc.). Types of Records include:

2.1.1. Active Record: A Record that is currently serving a business or educational purpose.

2.1.2. Archival Record: A Record that has permanent or historic value, is Inactive, and is not required for current business purposes. Archival Records are maintained by the division or department where they were created.

2.1.3. De-Identified Record: De-Identified Records are those from which Personally Identifiable Information has been permanently and irretrievably removed. Data that is de-identified is usually "rolled up" or aggregated for business or reporting purposes.

2.1.4. Electronic Record: A Record kept in a digital format. These include, but are not limited to, emails, word processor documents, spreadsheets, databases, HTML documents, PDF files, scanned or imaged documents, audio and video recordings, and any other type of file held on an electronic storage medium or cloud storage service.

2.1.5. Inactive Record: A record that is (i) not an Active Record, but still must be retained pursuant to the Records Retention Schedule, law, rule, or policy provision; or (ii) is no longer required to be retained but has not yet been destroyed.

2.2. Email System: The hardware, software and network used to provide a uniform email address, email functionality and efficiency to AHEC Users, primarily for use to carry out the business of the institution.

2.3. Legal Hold: An indefinite period during which all Records that are related to any pending or reasonably expected audit, inspection, governmental investigation, claim, lawsuit, or other official process must be retained, and not be modified, deleted or disclosed except upon the direction of the General Counsel.

2.4. Personally Identifiable Information (PII): Information that, if disclosed alone or in combination with other available information, would make it possible to identify an individual to whom the information pertains. This includes items such as a social security number; a personal identification number; a password; an official government-issued driver's license or identification card number; passport number; biometric data, such as that defined in Colorado Revised Statutes (C.R.S.) § 24-73-103(1)(a); an employer, student, or military identification number; a financial transaction device as defined in C.R.S. § 18-5-701(3); financial/account information; AHEC ID photo; class and work schedules; residency status; and age, birth date and place of birth.

2.5. Records Retention Schedule: A categorical listing of proper Retention Periods for Records. AHEC follows the State of Colorado, Department of Personnel and Administration, State Archives Records Management Manual, Schedule 8 (Higher Education) as its Records Retention Schedule.

2.6. Retention Period: The length of time a record needs to be maintained to satisfy the purposes for which it was created and to fulfill the legal, fiscal, and administrative requirements of AHEC and external agencies. The Retention Periods for specific Records are defined in the Records Retention Schedule. All Retention Periods are based on the fiscal year, from July 1 through June 30, and are in addition to the current year. For example, a three-year Retention Period means a document created this year should be kept until June 30th and then three additional years.

2.7. Sensitive Information: Includes both AHEC data that is not publicly available, and PII that through unauthorized disclosure may adversely affect an individual and/or AHEC. Examples include social security numbers, health information, financial information including credit card numbers, personnel and student performance information, proprietary research and academic information, student and staff ID photos, and personal location information including IP address.

2.8. System of Record: An information storage and retrieval system that is the authoritative source for a particular data element.

2.9. User: Any person having access to the Email System and provided with an AHEC.edu email address and account.

3. POLICY

3.1. All AHEC departments and offices maintain AHEC Records in physical format such as paper and photographs, and in digital formats using AHEC's systems, software and databases. AHEC is committed to the proper retention, storage, security, retrieval, and disposal of such Records in order to meet legal requirements, optimize use of space, minimize cost, and secure AHEC data.

3.2. All AHEC Records are the property of AHEC, even when they are in the possession of individuals, and must not be permanently removed from their appropriate location at AHEC nor destroyed other than as provided in this policy. AHEC Records are to be used for official AHEC business purposes, and not for personal use.

3.3. Unless otherwise specified in an applicable law, regulation, policy, or procedure, all AHEC Records shall be retained in accordance with the applicable Records Retention Schedule, regardless of their format. For Records that are not addressed in the Records Retention Schedule, or for assistance with Retention Periods, please contact the Legal Department, 900 Auraria Parkway, Tivoli 325, Denver, Colorado 80204, 303.556.2332.

3.4. AHEC Records should be retained only so long as they are valid and useful for legitimate AHEC business purposes, or as specified in the applicable Records Retention Schedule (whichever is longer). Inactive Records should not occupy office, storage, or computer space. Those responsible for Records must dispose of them in accordance with this policy when the specified Retention Period has expired.

3.5. **Important rule regarding Records related to pending audit, inspection, or litigation (Legal Hold):** Records whose Retention Period has expired must nevertheless be retained if related to any pending or reasonably expected audit, inspection, governmental investigation, claim, lawsuit, or other official process. Failure to hold and preserve Records under such circumstances is a serious matter that may expose a person to AHEC discipline, and/or civil or criminal liability. Any Record that is subject to a Legal Hold shall be retained, regardless of the expiration of its Retention Period, until disposition of the Record has been approved by the Legal Department. Records subject to Legal Hold shall not be modified, deleted or disclosed to any person or entity except upon the express

direction of the General Counsel. For further guidance and instruction on retention and disposition of such Records, contact the Legal Department.

3.6. Records in physical format that contain Sensitive Information or PII must be protected. Reasonable measures must be taken to prevent unauthorized access to these Records. Such methods may include locked file cabinets, locked office doors, and other security systems provided by AHEC.

3.7. Electronic Records should be stored on secure AHEC servers and devices that are password-protected in accordance with information technology security policies and procedures. All Records with Sensitive Information or PII must not be stored on portable media (such as CDs and portable drives). If a Record is stored in a System of Record, it should not also be stored locally, with exceptions for credit card transaction records and Procurement Card records.

3.8. Any breach of security exposing physical or Electronic Records to unauthorized release must be reported immediately to the Legal Department.

3.9. Digitization of Records

3.9.1. Most physical Records can and should be converted to an electronic format for purposes of storage, access, and subsequent destruction. With some exceptions, once digitized, a physical Record no longer needs to be retained, and should be destroyed in accordance with this policy, after assuring that the digitized Records are complete and there is no longer a need for the physical Record. Exceptions include:

- Original real property Records, contract documents and other Records that, in the judgment of the General Counsel, should be retained in their original form.
- To comply with Federal Acquisition Regulation 4.703(c)(3), which states, "the contractor or subcontractor retains the original Records for a minimum of one year after imaging to permit periodic validation of the imaging systems," original Records related to federal contracts are stored for one year after digitizing.
- Financial Records related to federal grants must be retained for a period of three years from the date of submission of the final expenditure report, or, for federal awards that are renewed quarterly or annually, from the date of the submission of the quarterly or annual financial report, respectively, unless a longer period is specified by the granting agency. 2 C.F.R. § 200.334.

3.9.2. Digitizing a Record does not alter its Retention Period. Just like paper Records, Electronic Records must be disposed of in accordance with this

policy when their Retention Period has expired. Once digitized, the Record becomes subject to AHEC's information technology security policies and procedures.

3.9.3. In order to assure that Records are properly digitized, and before disposing of the paper records, the responsible department should develop a plan to assure that digitization was accurate and complete, and in the appropriate format. Portable Document Format (PDF) is a file format intended to be suitable for long-term preservation of page-oriented documents and is the default format for all Inactive Records.

3.10. Disposition of Records

3.10.1. Records disposition is the final phase in a Record's lifecycle. It normally involves destruction, but, on rare occasions, the disposition may be to transfer the Record to another state or federal agency. Known requirements are listed in the Records Retention Schedule.

3.10.2. All AHEC departments and offices are strongly encouraged to conduct an audit of their Records at least annually to determine whether any such Records have reached the end of their Retention Period and should be disposed of in accordance with this policy.

3.10.3. Records should be destroyed promptly after the end of their Retention Period unless there is a continuing legitimate business need to retain them.

3.10.4. The approved method of destroying physical Records is by shredding to the current security standard for Sensitive Information, rendering the Records permanently irretrievable and illegible.

3.11. Electronic Records must be permanently erased so that they cannot be recovered by any means or device. Simply deleting them is not enough, as data often can be recovered after deletion using specialized tools and techniques. Portable physical media, such as CD-ROM disks, tapes, optical disks, memory sticks, memory cards, etc., should not be used for records containing Sensitive Information or PII, but, when they exist, they must be transferred to the Information Technology Department for proper disposal in accordance with applicable security policies and procedures. This includes computer hard drives (including servers) being removed from service at AHEC. Such items should never be transferred to another entity nor permitted to be converted to personal use, without reformatting of the disk(s). All hard drives considered to be e-waste must be reformatted, degaussed, or destroyed through a certified process. Units utilizing cloud-based storage must first have a security review and approval from AHEC Information Technology, and then work with the vendor to arrange for data to be purged after the expiration of

the Retention Period. The responsible department must receive documentation/evidence that destruction is complete.

3.12. Email Monitoring and Retention:

3.12.1. Monitoring of Email System: AHEC at all times has the right to monitor and read all emails generated, sent or received by the Email System, for the official business and legal purposes of the institution including, but not limited to, audits, investigations, and legal matters. Only persons authorized by the Director of Information Technology or the General Counsel shall monitor or read emails that are not generated by, sent to or received by such persons. Due care shall be taken to maintain confidentiality of messages monitored or read according to this section, except as required by law, audit, investigation, or other such circumstances.

3.12.2. Public Records: All employees of AHEC are advised that emails generated, sent or received in the Email System may be public records subject to disclosure under C.R.S. § 24-72-203.

3.12.3. Deletion of Emails: Emails generated, sent or received in the Email System should be deleted by the User when they are no longer necessary for the business purposes of the institution. Deleted email folders will be automatically emptied after 60 days. This section shall not apply to email messages that are subject to a Legal Hold, which shall be preserved (and not held in a deleted items folder subject to being emptied) until advised by the General Counsel as to disposition.

4. APPROVAL AND ADOPTION

This Policy has been reviewed and approved by the Board of Directors for the Auraria Higher Education Center.

Date: May 15, 2024

Approved by: */Tracy Huggins/*
Chairperson of the Auraria Board