University of Kentucky | Human Resources
Office of the Vice President

MEMORANDUM

DATE: July 22, 2025

TO: All Human Resources staff

FROM: Melissa Frederick
Vice President and Chief Human Resources Officer

SUBJECT: HR's Professional Standards: Sensitive and/or Confidential Information Agreement

As HR employees, each of you has access to sensitive and/or confidential information (university employee wages, criminal history, performance evaluation scores, applicant statuses, employment eligibility statuses, standing with the university, health information, as well as general information such as Social Security number and home address). The purpose of this agreement is to ensure you understand the professional standards within HR regarding sensitive and/or confidential information. Your principal obligations in this area are explained below. You are required to read and to abide by these professional standards as well as complete university-provided data security and confidentiality training as directed by your supervisor.

Human Resources professional standards regarding confidential and/or sensitive information agreement

Accessing, sharing and changing information

- I will protect UK confidential information in any form. I will follow UK policies, procedures and other privacy and security requirements.
- UK Public Relations & Strategic Communications provides services to the university that include internal and external communication, media relations, public relations counseling, crisis management, web design, and the writing, editing and design of university publications. The AVP and Chief Communications Officer of that office shall be the official spokesperson for the university. All media inquiries shall be directed to Public Relations & Strategic Communications. All university publications in any medium shall be approved by Public Relations & Strategic Communications.
- I will access, use and disclose sensitive and/or confidential information only as necessary to perform my job functions. This means, among other things, that:
    1. I will only access, use and disclose information available to me through my daily work, work location, departmental systems and/or the HRIS system as authorized and required to do my job.
    2. I will not in any way access, use, divulge, copy, release, sell or alter any information available to me through my daily work, work location, departmental systems and/or the HRIS system for either my own or another's personal interest. This includes via any medium such as telephone, video, email or social media.
    3. I will only access confidential information at remote locations with consent from my supervisor and, if allowed to remotely access confidential information, I am responsible for ensuring the privacy and security of the information at any location (e.g. home office, mobile devices, etc.).

4. I will not disclose any confidential information when my work or service at UK ends, nor will I take any confidential information with me when I separate or terminate.

Disposal and handling of paper documents

- I will follow the appropriate process for handling and disposing of confidential information.
    1. Any documents containing Protected Information (PI) or Personal Health Information (PHI) must be disposed of immediately after use in a locked blue confidential recycle bin. Those documents may not be placed in any open recycling container.
    2. I will only dispose of paper with sensitive/confidential information in the locked blue recycle bins.
    3. I will keep any paper documents with sensitive and/or confidential information out of the line of sight of any individual and unavailable to anyone who does not have a legitimate need to know.

User IDs and passwords

- Because all my user IDs and passwords are equivalent to my signature, and because I am the only person authorized to use them, I agree to the following:
    1. I will not share my user ID and password with anyone as outlined in the UK Computing Policy.
    2. I accept responsibility for all activities undertaken using my passwords, access codes and other authorizations.
    3. I will inform my supervisor and system administrator if I think someone knows or may use my password or if I am aware of any possible breaches of confidentiality at UK Human Resources.
    4. I understand that my user ID will be deactivated upon notification to Information Technology Services if I am no longer employed by UK Human Resources or when my job duties no longer require access to the computerized systems.
    5. I understand that HR management, as well as others in Information Technology Services, have the right to conduct and maintain an audit trail of all access to sensitive and/or confidential information.

I understand that any fraudulent application, violation of confidentiality or any violation of the above provisions, and the example of violations of these professional standards (see attached document), may result in corrective action, including loss of system and information access privileges, as well as other appropriate corrective action up to and including termination of employment and/or affiliation with the University of Kentucky.

My signature below indicates that I have read, accept and agree to abide by all the terms and conditions listed in this agreement and agree to be bound by it.

Signature: _____ Date: _____

Printed name: _____

Job title: _____

Example Violations of HR Professional Standards
Regarding Sensitive and/or Confidential Information
What you should not do

These are examples only. They do not include all possible breaches of sensitive and/or confidential information covered by this agreement.

Accessing information that you do not need to know to do your job:

Browsing open positions through the Hiring Official portal for personal interest.

Reviewing applications for positions for personal interest (it is ONLY appropriate to review positions for personal interest through the Job Seeker portal).

Reviewing another University employee's personal information including performance evaluation scores, corrective action, beneficiaries, health diagnosis/medications, retirement investments, etc. without a job-related reason (i.e. researching PE scores for a hiring official).

Sharing, copying or changing information without proper authorization:

Discussing another University employee's personal information such as PE scores, history of corrective action, health diagnoses/medication, retirement investments, etc. with anyone for non-work-related reasons.

Changing an individual's status either to or from ineligible for hire without proper authorization.

Discussing sensitive and/or confidential information in a public area such as a hallway, waiting room, elevator or cafeteria.

Taking pictures, discussing personal information, etc. with UK student athletes who are being provided a service in HR during work hours.

Improper disposal and handling of sensitive and/or confidential information on paper documents:

Disposing of paper documents with sensitive and/or confidential information in the open blue recycle bins or trash cans without shredding first.

Allowing someone who does not have a need to know view sensitive and/or confidential information.

Carelessness or misuse of User IDs and Passwords:

Being away from your desk while you are logged into a departmental system and/or SAP.

Allowing anyone to use your User ID and/or Password to access a departmental system and/or SAP.

Allowing anyone who does not have access to use your access to a departmental system and/or SAP after you have logged in.