Email Provisioning, De-provisioning, and Use Policy

Policy Number	4-016.1
Responsible Authority	Vice President for Information Technologies & Resources
Initiating Authority	Vice President for Information Technologies & Resources
Effective Date	10/04/2018
Date of Origin	12/13/2017

APPLICABILITY/ACCOUNTABILITY

This policy applies to all persons and entities that are provided an account in the university's electronic mail systems (i.e., Office 365 or Knights Email).

POLICY STATEMENT

Email is a key communication resource provided by the university for the benefit and use of its employees, students, and authorized others. All email users have the responsibility to use their university-provided email account in an ethical and lawful manner. UCF currently utilizes two official enterprise email solutions: a cloud-based system utilizing Microsoft's Office 365 (O365) for faculty and staff members for university business use and a separate O365 instance for students (Knights Email).

A copy of this policy shall be provided to all employees at the beginning of their employment at UCF. Any violation of this policy and procedures may result in loss of email privileges.

DEFINITIONS

Deleted account. An email account that has been purged from Office 365. Prior to deletion, contents of an employee account must be copied to a secure location to meet applicable records retention requirements.

Disabled account. Email account status that prevents the user of the account from accessing it. This account status can be changed by UCF IT email administrators or the Information Security Office.

Employee. A person who has been officially hired by UCF and has an employee record in the PeopleSoft HR system.

Enterprise Resource Planning System (ERP). PeopleSoft Student Administration, Human Resources (HR), or Financials systems: ERP is the authoritative source of information on Student, HR and Financials data, and identity data on all persons and entities affiliated with UCF.

Expired account. Email account status that prevents incoming email from being accepted. After six months of expired status the account is deleted. This account status can be changed by UCF IT email administrators or the Information Security Office.

Knights Email. UCF's student email system, supported by a distinct instance of Office 365. Students and current employees may obtain an account at no cost for personal use. Knights Email is the official communication channel for messages from university offices to students.

Non-Employee. A person affiliated with, but not officially employed by UCF.

Office 365 (O365). An email service offered by Microsoft Corporation. Office 365 is the email platform supporting UCF's enterprise email service and also Knights Email for students.

Phishing. An attempt to acquire sensitive information such as usernames, passwords, and credit card numbers, often for malicious purposes, through electronic communications, such as email or text messages.

Pre-Employment. The status of a person who has accepted employment at UCF, and is provisioned in the ERP system, but whose official start date has not occurred.

Retiree. An individual who has completed all steps necessary to retire from the university and is officially listed in the ERP system as a Retiree.

Spam. Unsolicited and undesired electronic messages containing advertisements for products or services.

Sponsored Account. A computer or email account created for individuals that do not fit standard employee or student roles, such as consultants, contractors, guests, courtesy appointees, etc.

Student. A person who has been admitted into full-time, part-time, or transient student status and who has a student record in the PeopleSoft student information system. See policy 4-010 Student Email for further details.
University Business. In the context of this policy, electronic mail messages that a person covered by this policy may send or receive in the conduct of their university responsibilities.

GENERAL POLICY

Email Data Ownership

The university owns all university email accounts in all Microsoft Office 365 instances. The content in the faculty and staff O365 instance is owned by the university. University business must be conducted using the Microsoft Office 365 faculty and staff instance.

The Knights Email system is for personal use, and therefore the content is personally owned. All email content in O365 instances is subject to copyright and other intellectual property rights under applicable laws and university policies.

Email Privacy and Right of University Access

The university will make every attempt to keep email messages secure; however, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through university email accounts. Under certain circumstances, it may be necessary for university IT staff or other authorized university officials to access university email accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents or investigating violations of this or other university policies; and, in the case of Microsoft Office 365 Accounts, violations of Microsoft's Acceptable Use Policy or the university's contracts with Microsoft. University IT staff or university officials may also require access to a university email account in order to continue university business where the university email account holder can no longer access the university email account for any reason (such as death, disability, illness, or separation from the university.) Such access will be on an as-needed basis and any email accessed will only be disclosed to individuals who have been properly authorized and have an appropriate need to know or as required by law. The university may access the contents of email accounts for purposes of e-discovery, or officially sanctioned investigations. All email users are bound by the appropriate acceptable use policies of both the university and Microsoft.

Data Retention and Purging

Email messages held in the O365 accounts for faculty and staff are subject to university's storage and email retention policies. O365 mailboxes are set to maximum storage size of one hundred gigabytes and ten years' retention. Any email over the ten-year period will be automatically purged, but may be archived by the account holder prior to the end of the ten-year retention period.

Email Record Retention

It is the responsibility of employees to preserve university records, including emails or instant messages in particular circumstances: 1) those who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed, 2) a subpoena has been served or notice of same has been given, 3) records are sought pursuant to an audit or similar pending or possible investigation, and 4) public records retention as required by Florida statutes or federal agencies.

Appropriate Use and User Responsibility

Highly restricted data, as defined by policy 4-008.1 Data Classification and Protection, must not be stored or transmitted within the university email system unless the data is encrypted. Restricted data, as defined by policy 4-008.1 Data Classification and Protection, may be transmitted or stored within the university email system without data encryption. Sending highly

restricted or restricted data from the university email systems to a non-university email system without data encryption is prohibited. Refer to the university's policy 4-008.1 Data Classification and Protection for further definitions and protections on restricted and highly restricted data.

Please refer to policy 4-006.1, Broadcast Distribution of Electronic Mail, for the university's requirements on mass email communications.

In order to prevent the unauthorized use of email accounts, the sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with this policy.

All incoming email is scanned for malware and spam. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is not possible to guarantee protection against all spam or malware, nor is it possible to prevent blocking of certain legitimate messages. It is therefore incumbent on each individual to use proper care to prevent the spread of malware. In many cases, messages containing or pointing to malware or phishing content appear to be sent from a friend, coworker, or other legitimate sources. Users should not click on links in an email message or open attachments unless the user is certain of the nature of the message and the sender. Suspicious emails should be forwarded, as an attachment, to sirt@ucf.edu where they can be investigated.

Personal Email Accounts
To avoid confusing official university business with personal communications, and to adhere to Florida public records laws, employees must not use non-university email accounts (e.g., personal Hotmail, Yahoo, or Gmail accounts) to conduct university business. Forwarding university business related email to a non-university personal email account is not permitted in order to prevent potentially sensitive university information from being sent to external, non-secure email systems.

PROCEDURES

Email Account Creation

Employees

Upon completion of the hiring or pre-employment process, and when an employee record is created in the Human Resources system, each employee becomes eligible for an email account. Creating an email account is initiated through an electronic form by the department's Human Resources Liaison, or delegate, and is based on the employee's role and relationship with the university. Email accounts are created based on the official name of the employee as reflected in the Human Resources system.

The standard format for an email account is: firstname.lastname@ucf.edu. Faculty and staff can establish an alternate, or alias, account name by using the self-service process in the myUCF portal.

Faculty and staff members can create a Knights Email account in the Knights Email instance for general personal use by using the online form at http://knightsemail.ucf.edu.

Once student applicants are matriculated, the student becomes eligible for a Knights Email account. Students use the above university-provided provisioning application to create their customized Knights Email account.

When a student is employed by the university (e.g., part-time employment, GTA, etc.), an email account may be requested by the HR Liaison in the O365 faculty and staff email system for the purposes of conducting university business.

Sponsored Accounts

University employees may request a UCF Sponsored Account and an associated email account. Sponsored account requests are reviewed on a case-by-case basis for individuals who are not UCF faculty, staff, or students. Sponsored accounts and online resource access can be requested using the forms and procedures found on the Service Desk web page. Sponsored accounts are established for one year and must be renewed annually.

Departmental Email Accounts

Requests for shared departmental accounts will be accommodated, but require designation of an account holder who will administer the addition, deletion, or modification of users within the account, as well as manage the account as per these guidelines.

Granting Access

The university may access the contents of email accounts for purposes of e-discovery, or officially sanctioned investigations at the request of the chief compliance and ethics officer, chief audit executive, or Office of the General Counsel.

Active Employees and Students

Request for access to an active employee's email account requires approval from the provost, chief compliance and ethics officer, chief audit executive, or Office of the General Counsel.

Former Employee

Request for access to a former employee's email account requires approval from the previous manager and approval from the dean or director of the employee's college or administrative department.

Email Account De-Provisioning

Notwithstanding the following procedures, university executives (e.g., president, provost, Office of the General Counsel, etc.) reserve the right to revoke email privileges for cause at any time.

Faculty and Staff who leave before retirement

Faculty and staff members who leave the university will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice. Upon request, automatic replies will be added to the email account to notify senders of the former employee's status and/or new contact information. An email account may also be assigned to a manager, or delegate, upon appropriate approvals. Contents will remain in the account's mailbox as required by current records retention requirements.

Sponsored Accounts

Sponsored accounts must be renewed annually. Sponsored accounts will become disabled if the sponsor of the account fails to renew the account through the sponsored account process. Once disabled, an email account can be re-activated upon sponsor request.

Retired Faculty and Staff

Faculty and staff members who have retired from the university will be permitted to retain a university email account as described in UCF policy 3-001.2 University Benefits for Retired Employees and the current UCF-UFF Collective Bargaining Agreement.

Active Students and Alumni

Knights Email accounts are currently not de-provisioned. Students who have graduated from the university will be permitted to retain their email privileges if the account continues to be actively used. In the event the university terminates or otherwise ceases its contractual relationship with Microsoft regarding the Knights Email system, all accounts will be deleted. Users will be given the option of downloading their data prior to deletion.

Expelled Students

If a student is expelled from the university, email privileges may be terminated immediately at the direction of the Office of Student Rights and Responsibilities.

RELATED INFORMATION OR DOCUMENTS

Further information regarding Microsoft's policies on Acceptable Use, Terms of Use, Privacy and Trademarks can be found on the Microsoft Acceptable Use page

UCF Policy 2-100.5 Florida Public Records Act—Scope and Compliance policy

UCF Policy 2-103.2 Use of Copyrighted Material policy

UCF Policy 3-206.5 Credit Cart Merchant Policy

UCF Policy 4-007.1 Security of Mobile Computing, Data Storage, and Communication Devices policy

UCF Policy 4-001.1 Retention Requirements for Electronic Mail

UCF Policy 4-002.2 Use of Information Technologies & Resources Policy

UCF Policy 4-006.1 Broadcast Distribution of Electronic Mail

UCF Policy 4-010 Student E-Mail

UCF Policy 4-209 Export Control Policy

UCF Policy 4-014 Procurement and Use of Cloud Computing and Data Storage Services

---

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 2-105.2

Initiating Authority: W. Scott Cole Date: 10/2/18

University Policies and Procedures Committee Chair: Date: 9/28/18

President or Designee: Dale Whittaker Date: 10.4.18

History 4-016 12/13/2017