President's Council
Guidelines & Protocols

Protocol/Guideline Title: UVU Employee Email Guidelines		
Responsible Office: Office of Information Technology		
Date Approved by President's Council: 5/9/2019		
UVU Web Host Page: https://www.uvu.edu/policies/guidelines/guidelines.html		
UVU Web Pages that Link to Host Page:		
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.

The following is not official university policy but rather a guideline used to facilitate the internal actions of the University or a particular unit within the University. Guidelines are not binding on the University and may be amended by the University at any time. A guideline, such as the one to follow, does not establish any contractual rights or obligations between the University and any individual.

President's Council
Guidelines & Protocols

Executive Summary

These guidelines define the appropriate use of and access to Utah Valley University (UVU) email services by faculty and staff employees ("employees").

Related Utah Statute

UCA 63G-2-101 *Utah Government Records Access and Management Act (GRAMA)*

Related Utah Board of Regents' Policies

Utah Board of Regents' Policy R840 *Institutional Business Communications*

Related University Policies

UVU Policy 441 *Appropriate Use of Computing Facilities*

UVU Policy 443 *Ethics in Computer Usage*

UVU Policy 445 *Institutional Data Management and Access*

UVU Policy 446 *Monitoring and Review of Employee Electronic Communications or Files*

UVU Policy 451 *Retention of Electronic Files*

General Principles

UVU recognizes that the principles of academic freedom, shared governance, freedom of speech, and privacy of information hold important implications for electronic communication and email services. These guidelines reflect those principles within the context of UVU's legal, operational, and administrative obligations.

UVU provides employee email and similar services to faculty and staff for official university business. UVU encourages the use of email services to share information, improve communication, and exchange ideas to advance UVU's mission in adherence to the principles of conduct in this guideline. The University expects employees to comply with state and federal laws, all UVU policies, and accepted standards of professional and personal courtesy and conduct. Immediately upon termination from the University, employees lose access to the email system, and to all contents of their accounts. Pursuant to Utah Board of Regents' Policy R840, employees shall use only their assigned UVU email account (uvu.edu) when conducting university business, and shall use university email in conformance to these general principles. Employees shall not use non-UVU email accounts for university business.

Security, Privacy, and Confidentiality

University Property and No Expectation of Privacy

All electronic messages, accounts, and addresses associated with the University are the property of UVU. The University owns all messages, files, and documents located on university information resources, including those that are personal. All content located on university information resources may be subject to open records requests, and may be accessed by the University in accordance with

policy. For these reasons, employees should have no expectation of privacy while using their assigned UVU email account, university-owned hardware, software, systems, or other technology-related property. UVU does not routinely inspect, monitor, or disclose electronic communications, files, or similar data, although it reserves the right to do so in situations such as, but not limited to, authorized investigations or suspected policy violations.

Public Record

Email, whether or not it is created or stored on UVU-owned equipment, may constitute a public record under Utah's *Public Records Act (GRAMA)* or be subject to mandatory disclosure under other laws, including laws compelling disclosure during the course of litigation. Employees should be aware that even incidental, non-work-related personal email residing on UVU equipment may be subject to GRAMA and similar laws.

Employees are responsible for ensuring that all electronic messages or files that are considered university business records are maintained on university information resources in accordance with all appropriate record retention requirements defined by university policy and by GRAMA.

Confidentiality

UVU strives to provide secure and reliable email services. However, the University cannot guarantee confidentiality of email. Confidentiality may be compromised by:

1) Technical problems or human error resulting in the unintended distribution of email;
2) Compromised passwords used for unauthorized access; or
3) Interception of messages during transmission across the internet or local networks.

Therefore, employees using UVU email services should exercise extreme caution when using email services to communicate confidential or sensitive matters. If necessary, employees should use whatever methods are available to them to secure confidential emails, such as password-protecting files, encrypting messages, etc. For more information on how to secure confidential emails, contact IT@uvu.edu.

Unauthorized Disclosure

State and federal law and UVU policy require that certain records remain confidential, including but not limited to, student records, peer review records, and certain personnel information. Therefore, employees using UVU email services are prohibited from transmitting, seeking out, using, or disclosing confidential information without proper authorization. When employees are authorized to transmit, use, or disclose confidential information through UVU email services, they must take appropriate precautions, including the use of encryption technologies or password-protected files to protect the confidential information.

Incidental Disclosure

During the performance of their duties, Information Technology (IT) personnel may need to observe transactions, address information, or messages to ensure proper functioning of the email or support systems. Except for the purposes stated, IT personnel are not permitted to intentionally view the contents of email messages, transactional information not germane to their purposes, or

disclose to others what they have seen. The right of authorized personnel to view email is limited to the least intrusive level of inspection necessary to perform assigned duties.

Removal of Information

UVU reserves the right to delete data remotely on devices that connect and download information from university email and related systems. This may include inadvertent removal of personal information from an individual's personal device by the email remote wipe process.

Employees should be aware that the University may filter, block, and/or remove potentially harmful messages or payloads from electronic messages.

Access Restrictions

Access to UVU email and similar services is a privilege that UVU may restrict wholly or partially without prior notice and without the employee's consent when there is reason to believe that violations of law or UVU policy have occurred, when an employee is suspended, or when other urgent or compelling circumstances arise.

Employees, including supervisors, are not authorized to access the electronic messages of another employee or terminated employee without their consent unless there is a business justification authorized by the Chief Information Officer (CIO) (or the CIO's designee), the Associate Vice President of Human Resources (AVP HR) (or the AVP HR's designee), and the General Counsel (or the General Counsel's designee). The CIO (or the CIO's designee) shall provide supervised access.

Rules of Conduct for Email Use

Personal Use and Access

Employees may use UVU email services for incidental personal purposes if that personal use complies with this guideline and Policy 441 and does not burden UVU with noticeable incremental cost(s) or interfere with the employee's job duties or other obligations to UVU.

Employees may access their University Account Mailbox using personal computing devices (smartphones, tablets, or other portable devices) so long as they

- Comply with all university policies regarding data protection and confidentiality.
- Use passwords or equivalent security to protect their personal devices used for accessing University Account Mailboxes.
- Ensure that their personal devices support remote wipe or removal of email in the event of device loss or theft.

If their device is lost, stolen, or compromised, employees shall notify and work with the Office of Information Technology (IT) to protect university data.

Misuse for Political Purposes

In accordance with state statute, UVU prohibits employees from using their UVU email: (a) for a political purpose; (b) to advocate for or against a ballot proposition; or (c) to solicit a campaign contribution.

Representation

Unless they are authorized to do so, employees shall not give the impression they are representing or making statements on behalf of UVU or any unit of UVU. Where appropriate, an explicit disclaimer shall be included in the email unless it is clear from the context that the author is not representing the University.

False Identity

Employees shall not employ false identities or send email on behalf of other users unless specifically authorized to do so.

Unacceptable Use

Employees shall not use UVU email services for purposes that violate UVU policies or that involve unlawful activities, personal financial gain, political or commercial purposes not under the auspices of or for the benefit of UVU.

Employees shall not auto-forward incoming messages to accounts outside the employee email system. The employee email system does not allow automatic forwarding of messages outside of the employee email systems. Employees shall use discretion when forwarding individual messages or when "replying to all" due to the University's significant liability for messages not under UVU control.

Employees shall not share email address lists of employees or students without proper authorization.

Mass Emailing Process Approval and Limitations

Mass emailing must be approved as outlined by UVU policy and in compliance with the CAN-SPAM Act. Employees who send mass email without proper authorization will have their account disabled and the system administrator may retract the emails.

Employees sending authorized mass emails shall use the BC field to maintain the privacy of the recipients' email addresses.

All employees are authorized to email the people over which they have stewardship or a supervisory role. Emails to large groups that are outside of an employee's role must go through proper existing channels (like UVAnnounce), or must go through the approval process and must have an opt-out method as outlined in the CAN-SPAM Act.

The employee email system allows the maximum of 500 recipients per message and a maximum of 10,000 recipients per 24-hour period. Mass mailings attempted without prior OIT action may be blocked automatically by the filtering system. Official university contact information for the sender must be included in all distributed messages. Mass emailing from an outside system must comply with the CAN-SPAM Act and requires approval from the University Communications Committee and OIT or the emails may be blacklisted or blocked by university filters or firewalls.

Theft and Abuse

Applicable laws and UVU policies strictly prohibit theft or other abuse of computing resources and information. Such prohibitions apply to email and related services and include, but are not limited to, unauthorized entry, use of, transfer of, and tampering with unauthorized accounts and files;

interference with the work of others and computing facilities; and the transmission of materials that pose a direct threat to safety, violate discrimination or harassment laws or policies, contain confidential information, or violate intellectual property laws. Any suspected misuse should be reported to Human Resources, or via EthicsPoint (https://uvu.edu/audit/concerns).

Interference with Email Systems

Employees shall not use UVU email for purposes that could reasonably be expected to cause, directly or indirectly, strain on computing systems or unwarranted or unsolicited interference with another's use of email services. Such prohibited use includes but is not limited to the following:

1) Sending or forwarding chain letters;
2) Using list servers or similar broadcast systems to accomplish the widespread distribution of unsolicited email (spam); or
3) Resending the same electronic mail repeatedly to one or more recipients to interfere with the recipient's use of email services (letter bombing).

Account Life Cycle

New Employees

All employees will be issued an email (UVID@uvu.edu) account upon hire. Employees should also create an alias/preferred address (name@uvu.edu) at: https://ais-linux6.uvu.edu/idm/email/activate.php. Automated systems will create accounts based on the information created and maintained through HR processes in the BANNER System.

Employees on Leave

Employees are responsible for working with their supervisors before a short-term or extended leave to ensure business continuity concerns will be addressed during their absence. This could include configuration of an out-of-office/auto-response message or establishing appropriate mail forwarding rules to other institutional accounts.

Continuing Part-time/Adjunct Employees

Continuing temporary employees or employees with no terminating ePAF (such as adjunct faculty or hourly staff) may continue to have access to their email between work assignments and/or semesters. If departments do not want these employees to have access during these interim periods, the appropriate supervisor must submit a termination ePAF.

Account Termination: Supervisors' Responsibilities Related to Terminating Employees

Submit an ePAF

As soon as a supervisor knows that a notice of termination or a termination will occur, they are required to submit an ePAF for the terminating employee.

Determine Holds and Access

Before submitting an ePAF, the supervisor shall determine and report to IT any departmental needs for records retention or business continuity. The supervisor shall also determine and request from the applicable vice president any post-termination departmental consulting by the terminating employee that may require continued email access. The supervisor shall also consult with General Counsel (or General Counsel's designee) to determine any needs for litigation holds.

Requests for Auto-Reply Customizations

Supervisors or others who have a business need may request a change to the standard auto-reply message. Requests must be submitted to OIT and must include the business justification.

Business Continuity

University departments are encouraged to utilize general department contact information (phone numbers, email addresses, etc.) rather than employee-specific contact information for official business uses. This allows electronic communications to continue to be routed to appropriate staff without needing to notify others of changes in personnel.

Account Termination: Terminating Employees' Responsibilities

Removal of Personal Messages and Notification of Personal Contacts

Employees are responsible for removing all personal messages from their University Account Mailbox before their last date of employment. It is the employee's responsibility to notify any personal contacts of their new contact information.

Removal of University-related Content from Personal Devices and Non-University Accounts

Employees are responsible for removing all messages considered university business records from any personal accounts where information is forwarded or stored, as well as from their personal devices, such as smart phones, before the end of their employment.

Update Contact Email Address

Before their last day of employment, employees are responsible for updating BANNER with a current personal email address to ensure they can continue to receive communications from Human Resources.

Notify UVU of Data Retention Requirements

If a terminating employee determines it would be in their own or the University's best interest to request a legal hold, retention, or individual access, they must notify their supervisor or HR within 30 days of their termination date.

Major Role Changes

An employee who changes roles from a position with access to sensitive information to a position not requiring access to the same sensitive information may be required to change to a new email address and may lose access to their former email contents.

Account Termination: Post-Termination Access

Voluntary and Involuntary Termination

Employees who voluntarily leave UVU will have access to their email account until 5:00 p.m. on their termination date. Employees who are involuntarily terminated will have access to their email account suspended at the time they are informed of the termination. All incoming messages to the terminated employee's account will receive a generic auto-reply stating that the person is not currently employed by UVU.

Temporary Account Access by Supervisors after Employee Termination

Supervisors may request access to the information in a terminated employee's account for 60 days beyond the termination date. All email accounts and files of terminated employees will be deleted 90 days after the termination date, unless UVU places a hold on the account. As part of the termination process, supervisors will be notified of these dates and of their responsibilities listed in the Account Termination: Supervisors' Responsibilities Related to Terminating Employees section of this document.

Supervisors should contact the AVP HR (or the AVP HR's designee) to request access, providing business justification for the access. The AVP HR (or the AVP HR's designee) will consult with the CIO (or the CIO's designee) and the General Counsel (or the General Council's designee) to determine if authorization is warranted. If authorized, the supervisor (or the supervisor's designee) will be granted access for a limited amount of time under supervision by the CIO (or the CIO's designee).

Temporary Account Access by Terminated Employees

In rare circumstances, terminated employees, or others properly authorized by HR, the employee, or OGC, may request access to the information in the employee's account for 60 days beyond the termination date. All email accounts and files of the terminated employee will be deleted 90 days after the termination date, unless UVU places a hold on the account. As part of the termination process, exiting employees will be notified of these dates and of their responsibilities listed in the Account Termination: Terminating Employees' Responsibilities section of this document.

Requests for access should be addressed to the AVP HR (or the AVP HR's designee), providing justification for the access. The AVP HR (or the AVP HR's designee) will consult with the CIO (or the CIO's designee) and General Counsel (or General Council's designee) to determine if authorization is warranted. If authorized, the terminated employee (or requestor) will be granted access for a limited amount of time under supervised access by the CIO or the CIO's designee.

Post-Termination Email Privileges

Availability of my.uvu.edu Account

Terminating employees may request or retain an email account in the student email system @my.uvu.edu. Requests for these accounts should be directed to IT.

Ongoing Account Access by Terminated Employees

In exceptional cases, where there is a significant business need in UVU's best interest, terminated employees may request that UVU maintain their email address (address forwarding), or allow them

to retain access to their existing employee email account (retained access) for a limited period of time beyond 60 days. The request process is as follows:

1) Employee's supervisor must submit a request for the desired level of access (address forwarding or retained access) to the appropriate vice president. The request must include an explanation of the business need for the request.
2) The appropriate vice president will evaluate the request to determine if it is appropriate; if they approve the request, the vice president will submit the request to President's Council for approval.
3) If the request is approved by President's Council, the terminated employee shall: (a) not perform work on behalf of the university without payment for these consulting services, which must be detailed in a signed agreement between the University and the terminated employee; (b) have access only to information that permits the terminating employee to fulfill the significant UVU business need; (c) forward all applicable content to the appropriate person at the University; (d) sign an agreement detailing confidentiality and data privacy requirements and other duties and responsibilities related to their use of UVU email services; and (e) request a renewal for their post-termination email privileges every six months.

Address Forwarding

With address forwarding, UVU will maintain a terminated employee's email addresses, but all new messages will be forwarded to the terminated employee's personal email account. Any replies will be from the terminated employee's personal email address. With address forwarding, the terminated employee will not have access to the contents of their employee account.

Retained Access

The university may approve one of two options for retained access for terminated employees:

1) UVU will maintain all email addresses and account contents. The terminated employee will have the same access to their account contents as they did before their termination. The account will be within the existing employee email system; or
2) UVU will maintain some or all email addresses for the account but the terminated employee will not be able to access the content that existed before their termination date. The account will be within the existing employee email system.

Disciplinary Action

Violations of these guidelines may result in restriction of access to UVU information technology resources, in addition to appropriate disciplinary action, up to and including termination.

HISTORY		
May 9, 2019	Approved	President's Council