Lindsey Wilson College

Email Policy

Policy 02-20

Purpose
The purpose of this policy is to ensure the proper use of email accounts provided to faculty, staff and students using the College's domain name pursuant to an agreement between Lindsey Wilson College and Google, Inc. Electronic Mail is a tool provided by the College to complement traditional methods of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the account evidences the user's agreement to be bound by this policy. Violations of the policy may result in restriction of access to email and/or other appropriate disciplinary action.

Account Creation
Student, faculty and staff email accounts are created based on the official name as reflected in Human Resource, Payroll and Registrar records. Requests for mail aliases based on name preference, middle name, nicknames, etc. will be accommodated if possible but are not encouraged. Requests for legal name changes due to marriage, divorce, etc. should be directed to the Computer Center.

Ownership of Email Data
The college owns all email accounts under the Lindsey domain including information stored in the Google apps product.

Personal Use by Employees
While incidental personal use of a College-issued email account is acceptable, it is not encouraged or supported. When an employee leaves the College and the email account is terminated, business related emails may be directed to another recipient, but personal emails will not be forwarded. Conducting business for profit using a Lindsey email account is forbidden. The use of a College-issued email account for political activities (supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum) is forbidden. Solicitations other than for official College business are not permissible. Any use of a College-issued email account to represent the interests of a non-College group must be authorized by an appropriate College official.

Privacy and Right of College Access
While the College will make every attempt to keep email message secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages. Under certain circumstances, it may be necessary for the IT staff or other appropriate College officials to access 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 College policies, and violations of Google's Acceptable Use Policy or the College's contract with Google. IT staff or College officials may also require access to an email account in order to continue College business where the email account holder will not or can no longer access their account for any reason (such as death, disability, illness or separation from the College for a period of time or permanently). Such access will be on an as-needed basis and any

email accessed will only be disclosed to those individuals with a need to know or as required by law. Google also retains the right to access the Gmail accounts for violations of its Acceptable Use Policy.

Data Purging and Record Retention
Email messages on the Gmail Accounts will be subject to Google's purge policies, which may change from time to time without notice. Google currently provides the following guidelines for purging folders:

- Trash – 30 days
- Spam – 30 days

Employees must preserve College records, including emails or instant messages, if they have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed, a subpoena has been or will be served, or records are sought pursuant to an audit, a government investigation or similar circumstances.

Data Backup
All faculty, staff, and student email accounts are hosted through Google, and there are no restoration services offered for email accounts.

Expiration of Accounts
There are many situations where the length of email privileges or expiration of accounts will differ, as set forth below when an individual leaves the College. Notwithstanding the guidelines below, the College reserves the right to remove email privileges at any time. With supervisory approval, a grace period may be provided upon request for those who wish to transfer items from their LWC email account. Upon departure from LWC, the network account (provides Portal access) will be terminated, but email and other appropriate services will remain accessible through direct web links.

- **Faculty who leave before retirement** – Faculty who leave before retirement will have email privileges removed at the end of their last working day. If such separation is for cause, email privileges may be immediately suspended indefinitely without notice.
- **Staff who leave before retirement** – Staff members who leave before retirement will have email privileges removed at the end of their last working day. If such separation is for cause, email privileges may be immediately suspended indefinitely without notice.
- **Retired Faculty and Staff** – Faculty and staff who retire from the College will retain their email privileges indefinitely; however, if there is no usage for a period of one year, the email account may be removed.
- **Adjunct Faculty** – Adjunct Faculty will maintain email privileges for two academic years from the last term in which they taught, unless informed otherwise by the Vice President for Academic Affairs.
- **Students who leave before graduation** – Students in good standing may keep their email privileges indefinitely; however, if there is no usage for a period of one year, the email account may be removed.

- **A student who is dismissed** – If a student is dismissed from the College, email privileges will be terminated immediately or as directed by the Vice President for Student Services or designee.

- **Alumni** – Graduating students will maintain email privileges indefinitely; however, if there is no usage for a period of one year, the email account may be removed.

In the event the College terminates or otherwise ceases its contractual relationship with Google regarding the Gmail Accounts, users will lose email privileges in accordance with the terms of the Google contract. Notice will be provided as soon as reasonably possible.

Appropriate Use

When using email as an official means of communication, students, faculty and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, students, faculty and staff should not communicate anything via email that would not be appropriate or desirable to say publicly. Users of email shall not disclose information about students or employees in violation of College policies or laws protecting the confidentiality of such information.

No private personally identifiable information about College faculty, staff, students, alumni or other College members should be transmitted via email or stored in an unencrypted format. This includes but is not limited to Social Security number, bank account information, tax forms or other sensitive data.

Employees must have supervisory approval before being granted permission to email group announcements to students, faculty and/or staff.

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes as per these guidelines. In some cases where email messages generate a high number of responses due to the subject matter, it may be appropriate to utilize other types of social media.

User Responsibility

The College-issued email account is the official means of communication with faculty, staff and students. All users are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding College matters sent from an administrative office, faculty, or staff member is considered to be an official notice. Faculty, staff, or students who choose to use a different email account are responsible for receiving College-wide broadcast messages. An alternate method of checking College email is to utilize the forwarding feature, which can be set to forward mail to an individual's personal email account.

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 deemed to be authorized by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

Departmental Accounts

Requests for departmental accounts will be accommodated but require a designation of an account holder who will manage the account. The account holder must notify the IT department when the account is no longer needed or if it should change ownership.

Inappropriate Use

All Gmail Accounts, including those of faculty, staff, students, and alumni, are subject to Google's Acceptable Use Policy (http://www.google.com/a/help/intl/en/admins/use_policy.html). In addition, any inappropriate email usage, examples of which are described below and elsewhere in this policy, is prohibited. Users receiving such email should immediately contact the Computer Center. Examples of inappropriate communication include but are not limited to:

The exchange of email content that:

- Generates or facilitates unsolicited bulk commercial email;
- Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- Violates, or encourages the violation of, the legal rights of others or federal and state laws;
- Is for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- Alters, disables, interferes with or circumvents any aspect of the email services;
- Tests or reverse-engineers the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- Constitutes, fosters, or promotes pornography;
- Is violent, incites violence, threatens violence, or contains harassing content;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Misrepresents the identity of the sender of an email.
- Is otherwise malicious, fraudulent or may result in retaliation against the College by offended viewers.

Other improper uses of the email system include:

- The use or attempt to use the accounts of others without their permission.
- Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting);

- Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- Any conduct that is likely to result in retaliation against the College's network or website, or the College's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

These guidelines provide some examples of permitted or prohibited use of email. This list is not intended to be exhaustive but rather to provide some illustrative examples.

Spam & Virus

Although Google blocks known viruses and spam emails, it is impossible to protect against all spam and virus infected messages. It is, therefore, incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases viruses appear to be sent from a friend or coworker, therefore attachments should only be opened when the user is sure of the nature of the message. If any doubt exists, the user should contact the Computer Center. Messages that seem to come from IT requesting a username and password are spam. We will never request that information in an email. Many such messages have no contact name or phone number listed, which usually indicates that it is mass produced and not from a legitimate sender.

Any user with questions regarding proper email usage or accounts in general should contact the Computer Center at 270-384-8017.

Policy History:

Origination Date: 4/27/17

Revision Date: 4/25/19