Email Account Policy

Purpose

This policy outlines the guidelines for email use and management within the OWWL Library System ("the System").

Questions or concerns regarding this policy should be directed to the Executive Director.

Scope

This policy applies to all users of email services provided by the System.

Email Accounts

The System offers free email accounts for employees at System headquarters and Member Libraries. The accounts are intended to facilitate communication between the System, Member Libraries, and within the library profession.

The System does not provide email accounts for Member Library Boards, individual Trustees, treasurers, or volunteers.

Account Creation

Email accounts for Member Library staff must be requested by the library director or their designee using the Account Maintenance Request Form on OWWL Docs. An email account for a Member Library director must be requested by the library's Board President or the System's Executive Director.

After the creation of an email account, the user will be assigned an email training and has 30 days to watch and complete the training. If the training is not completed within 30 days, access to the email account will be revoked.

Account Deactivation

Upon the separation of staff from a Member Library, the library director or their designee must immediately notify the System via the Account Maintenance Request Form. This allows the System to deactivate the email account. Whenever possible, the notification should occur in advance of the date of separation to ensure that individuals who should no longer have access to System email are removed as users. A library's Board President is responsible for informing the System of the separation from service of a library director.

If necessary to ensure business continuity, directors can request to have the departing staff's email forwarded to the director's account for up to three months.

In limited circumstances, an incoming director may request temporary access to the contents of the previous director's mailbox to ensure business continuity.

Account Maintenance

To maintain a clean email database, the System will distribute a list of email accounts to each Member Library director on at least an annual basis. Directors are responsible for notifying the System immediately if staff on the list are no longer employed by the library.

Aliases

The System may assign email aliases to certain users, such as directors. Aliases allow users to send and receive email from additional addresses inside their primary email account. Aliases can be assigned to one person at a time.

In limited circumstances, new Member Library directors may request that the old director's email address be set up as an alias to ensure business continuity. This arrangement will last no more than six months.

Group Membership

All email accounts are added to the OWWL Library System mailing list.

Additionally, each library has a LIBstaff mailing list. Staff at each Member Library must have their email account added to their library's staff mailing list.

Email Use

Email accounts are to be used for library business and communications only. Personal use is not recommended as it may violate System and/or Member Library local policy.

Users with an OWWL email address are prohibited from using email for any illegal or unethical purposes. Email communication should be professional, respectful, and free from discriminatory or harassing language. All email users must uphold System and local library policies.

Auto-forwarding to move email from the System managed email system to a non-System managed email system is prohibited.

Email Management

Users are responsible for managing the contents of their own email accounts and ensuring that they comply with this policy.

Retention

For storage consideration, users should avoid retaining large amounts of email for long periods of time.

Email is not an appropriate place to retain library records; these records should exist outside of the System email system, and copies of those records must be retained by the library which originated them. Emails that the holder determines are of lasting value should be printed on paper and filed, or saved as a PDF to their computer or other digital storage media. Users should follow their local library's Records Retention policy as it applies to email communication.

In the course of conducting business, library staff may use email to communicate confidential information about patron accounts and library usage, including patron personally identifying information (PII). In the event of an email hack or breach, messages containing such information put the System and its Member Libraries at risk for litigation, as well as financial loss through legal and administrative fees and staffing costs related to dealing with such a breach.

To lessen this risk, some shared email accounts (circulation, reference, etc.) have a 35-day retention protocol. After 35 days, email messages will be automatically deleted. This automatic deletion protocol applies to emails within all folders on the account. Once the

emails are deleted, they are moved to a temporary holding folder on the System email server. After an additional 30 days, the emails are permanently deleted.

Shared print email accounts have a 1-day retention protocol. After 1 day, email messages will be automatically and permanently deleted. This automatic deletion protocol applies to emails within all folders on the account.

This retention protocol does not apply to shared email accounts that are forwarded to an individual's primary account, shared email accounts that are set up as an alias, and director email accounts.

Disposal

Users who send or receive email messages that contain confidential or sensitive information, such as PII, are expected to delete such messages from all email folders, including Inbox, Sent, and Trash, as soon as the email is no longer necessary for carrying out library business.

Storage Quotas

Email storage quotas will be implemented on each account to ensure adequate space for all users.

Users should regularly review and delete any unnecessary emails to conserve storage space. Users may request additional storage space by opening a support ticket.

Security and Confidentiality

Users must take appropriate measures to ensure the security and confidentiality of their email account.

Passwords

In accordance with the System's Systems Access and Confidentiality of Library Records Policy[1], passwords for email accounts should:

[1] https://owwl.org/system/systemsaccess

- Be randomly generated[2];
- Be at least 12 characters long;
- Be unique, meaning they are not reused for other accounts; and
- Contain some level of complexity.

Passwords should not:

- Consist of previously used passwords;
- Consist of passwords used for personal accounts.

Users should promptly change their email password upon receiving credible evidence that their password has become known by or disclosed to another party, or when requested to do so by their supervisor or the System's Computer and Network Services staff.

Sharing Accounts

Some email accounts are meant to be accessed by multiple staff, such as circulation, reference, and print accounts. However, individual users should not allow anyone else to use their email account.

Passwords to shared email accounts must be changed upon the separation of service of an individual who is no longer authorized to access that email account. The responsibility to ensure that passwords are changed ultimately rests with the library director.

Spam, Phishing, and Viruses

Incoming emails are scanned for viruses, phishing attacks, and spam. Suspected malicious messages are blocked from the user's inbox. However, it is impossible to guarantee complete protection from all malicious emails.

Users should exercise caution when interacting with emails that show signs of being phishing, spam, or infected by viruses. If any doubt exists, the user should contact the System's Computer and Network Services department by opening a support ticket.

Confidentiality

[2] Use a password generator to create a password. Password generators are often offered by password managers, like the generators offered by 1Password (https://1password.com/password-generator/) or LastPass (https://www.lastpass.com/password-generator).

The System will make reasonable efforts to maintain the integrity of email systems, but users should not regard email as a secure medium for the communication of sensitive or confidential information, such as patron PII. Users should exercise caution about sending sensitive or confidential information via email, and should limit any such communications to those with a legitimate need to know.

Accessing Email Accounts

The System has the ability and reserves the right to access email accounts when there is a legitimate need, including but not limited to investigating a data breach, responding to support tickets related to issues with the account, or as required by law.

Violations

Violations of this policy may result in suspension or blocking of email privileges when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the System email system, or to protect the System and its Member Libraries from liability. Suspected violations will be reviewed by the System's Executive Director and/or the Computer and Network Services Manager.

Approved: January 8, 2025