OFFICE 365/EMAIL ACCOUNT POLICY

Account Creation

Southwestern College Office 365 accounts are created for all current Students, Faculty and Staff based on the user's official name as reflected in our Student Information System. Requests for name changes must be made through the Registrar's office (for Students) or Human Resources (for Faculty/Staff). Requests for mail aliases based on another name (preferred, middle, etc.) are evaluated on a case-by-case basis.

Student Accounts

Student Office 365 accounts will be created starting approximately 10 days before the beginning of each term for Main Campus students and will be created approximately 3 weeks before the beginning of each session for Professional Studies students.

Faculty/Staff Accounts

Faculty/Staff Office 365 accounts will be created upon notification from Human Resources.

Other Office 365 Accounts

Southwestern College departments and other affiliated groups may request the creation of Office 365 accounts or distribution lists. These requests will be considered on a case-by-case basis. Departmental accounts must have a member of the Southwestern College community designated as the responsible party for the account. Departmental accounts will be periodically reviewed for continued use.

Affiliated Personnel

In some cases, persons closely affiliated with Southwestern College (alumni, vendors, etc.) may be granted the use of a college Office 365 account. Requests for these accounts will be reviewed on a case-by-case basis.

Account Retention

Student's Office 365 accounts are kept active for 1 year after the student is no longer enrolled in at least one course at the college. Upon deactivation of a Student's Office 365 account, the student will lose all access to all data (emails, OneDrive, SharePoint Online sites, etc.) associated with the account. It is the responsibility of the student to ensure that any data residing in the account is retained prior to deactivation.

Faculty/Staff Office 365 accounts will be removed upon notification from Human Resources. Requests to extend access to specific accounts must be made through Human Resources prior to termination. Upon deactivation of a Faculty/Staff member's Office 365 account, the user will lose all access to all data (emails, OneDrive, SharePoint Online sites, etc.) associated with the account. It is the responsibility of the employee's supervisor to ensure that any institutional data residing in the account is retained prior to deactivation.

Personal Email Accounts

In order to avoid confusing official Southwestern College business with personal communications, employees must never use non-SC email accounts (gmail, AOL, iCloud, etc.) to conduct Southwestern College business.

Privacy

While Southwestern College respects individual's right to privacy in communications, complete privacy of our email services is not guaranteed. Southwestern College does not routinely monitor or access the content of emails, though the college reserves the right to investigate use of college email services or disclose the content of individual emails with appropriate authorization.

SPAM & Phishing

Southwestern College currently has an anti-spam system that stops a vast majority of spam messages and viruses from reaching your inbox. Unfortunately, no anti-spam solution is perfect, and the spammers are always one step ahead of the anti-spam industry. Eventually, the industry will determine a pattern to block spam that slips through the filters. When this happens, our system will automatically be updated to block spam plaguing our campus.

Because malicious messages can and do reach user's inboxes, it is imperative that each individual use proper care and caution to prevent the disclosure of personal or college information. If an individual discovers that they have been a victim of a virus or phishing attack, Southwestern requires that the individual report the incident to the SC Helpdesk so proper precautions can be taken to prevent the spread of such attacks. In the event that a Southwestern College account is reported as compromised by an individual other than the account owner, the College will suspend the user account immediately and contact the owner of the account for resolution.