Culver Educational Foundation

User Account and Email Policy

Overview
Culver Educational Foundation's email services support the educational and administrative activities of the school and serve as a means of official communication by and between users and CEF. The purpose of this policy is to ensure that this critical service remains available and reliable, and is used for purposes appropriate to the CEF mission.

User Account Provisioning
CEF User Accounts are provisioned following all necessary approvals on the IT Request Form.

Permitted Use
CEF User Accounts and email should be primarily used for business purposes.

Incidental personal use of email is allowed with the understanding that the primary use be job-related, and that occasional use does not adversely impact work responsibilities or the performance of the network.

The following are prohibited:

- intentional and unauthorized access to another person's email;
- excessive personal use of email;
- inappropriate or illegal content such as offensive jokes;
- use of email for political or lobbying activities;
- engaging in illegal activities or harassment;
- encrypting personal emails and attachments;
- use of email to transmit materials in a manner which violates copyright laws.
- sending "spam", chain letters, or any other type of unauthorized widespread distribution of unsolicited mail;
- sharing credentials with other employees or non-employees

Mobile Devices
Culver email may be accessed via a mobile device

1. Via Internet browser with Culver Credentials; or
2. Microsoft Outlook app, provided that the device is authenticated on Culver's Microsoft Intune Company Portal.

In order for a Culver user account to be accessed via mobile device, the device must have a passcode set up on it. These requirements are enforced by system policies.
Culver account information will be remotely wiped if a mobile device is lost, stolen, or the employee departs Culver.

Email Signatures
To keep in line with Culver's brand, email signatures should be used on every email account and must be generated using this tool: https://www.culver.org/email-signature
Email backgrounds other than white should not be used.

Credentials
User Account password rules are governed by the CEF Password Policy. Passwords must not be shared with any other employee or non-employee.

Confidential Information
When sending confidential information (i.e. PII, PHI, student data, or employee data), the user should encrypt the message (Options > Permissions > Select encryption option).

Malware
CEF email users should be careful not to open unexpected attachments from unknown or even known senders, nor follow web links within an email message unless the user is certain that the link is legitimate. Following a link in an email message may execute code that can install malicious programs on the computer or network.

Identity Theft
Forms sent via email from an unknown sender should never be filled out by following a link. Theft of one's identity can result.

Monitoring
CEF reserves the right to read individual emails that were sent or received from Culver's email account and has the authority to access and inspect the contents of any equipment, files or email on its electronic systems.

Employee Departures
Any needed content (emails, files, etc.) should be obtained from the employee prior to the departure, when possible.

When a faculty or staff member departs, their email address is deleted on the last day of their employment. If anyone sends a message to that address, the sender will receive a message indicating that the account no longer exists.

An optional auto-reply may be added, upon request of the departing employee's manager, for a period of 2 weeks following the departure. The standard auto-reply message is:

We regret to inform you that (former employee) is no longer employed at Culver Academies. Please direct any future correspondence to (person responsible) at (person responsible email).

Forwarding of a user's email after their departure is prohibited.

The departing employee's immediate supervisor will gain access to their OneDrive account for a period of 30 days following the termination date.

Due to data retention restrictions, mailboxes may not be exported (i.e. to a .pst file) at any time.