

Campus Email Services

Access employee and student email, Sender Policy Framework.

- [Student \(Google\)](#)
 - [Access Student Email](#)
 - [Student Email Password Reset](#)
 - [Stop Student Everybody Emails](#)
- [Sender Policy Framework \(SPF\)](#)

Student (Google)

Access Student Email

Overview

MCC student email accounts are intended for school-related communication while you are an active student. Your account will be created for you, and you do not need to create a student email account.

These are instructions to access your student email.

Getting Started

- Go to [Student Email](#) or to www.mclennan.edu > I am a > Current Student. Click on **Student Email**. You can also log into gmail.com with your student email address.
- Your login username will be your email address: the first initials of your first name and last name, your 7-digit MCC ID number followed by @students.mclennan.edu.
- You will use the password you created for MyMCC or Brightspace.

Access to Email

Your Student Email account will be created within 2 hours of receiving your Acceptance Letter from McLennan Community College (MCC).

- Although your account will be created within 2 hours, trying to access within this 2 hour window may result in an error stating: your account does not exist.
- If you receive an error, please wait; your account will be created shortly.
- It is accessible within 24 hours or by the next business day.

MCC student email accounts are active up to 12 months after your last MCC course.

Benefits and Features

- customizable start page
- 15 gigabytes of space
- spreadsheet program

- presentation program
- MS Word compatible document editor
- Google chat

Resources

Need to reset your password?- [Forgot Password](#).

Policy

Your official McLennan Community College email account is provided through Google. All students, staff, and faculty will use their official college email addresses when conducting college business as per [MCC's Official Email Communication Policy](#).

Termination of Email Access

It is not recommended to use your student email for long-term personal use or to link it with third-party services such as: social media, medical portals, banking, etc.

- After a 12-month period without any active courses, your student email account and all associated data, including Google Drive, will be deleted.
- Upon leaving MCC, be sure to update any account, associated with or linked to your student email with your personal email address.

Student (Google)

Student Email Password Reset

Overview

This article covers changing your student email password.

Getting Started

The password reset link on Google Mail will not reset your student email password. You will get an error to contact your administrator. You can reset your student email password at [Forgot Password](#).

Stop Student Everybody Emails

Overview

MCC student email accounts are used to communicate important information to students, both individually and through campus-wide announcements. If you are a former student and still receiving these emails but would like these to stop, follow the steps below based on your situation.

Important Note

Emails sent to all student accounts will always reach all student email addresses. Since no mailing list is used, there is no way to remove an address from these announcements. It is not possible to opt out of campus-wide emails such as newsletters, technical alerts, or general student announcements. These messages are sent directly to all active student email addresses.

Getting Started

Choose the guide below that best applies to your situation.

Your Student Email is Logged into an Email App

If you are receiving unwanted notifications from your student email account on a device, log out of your student email on all apps where it is signed in. The process varies by app. Here are guides for common apps:

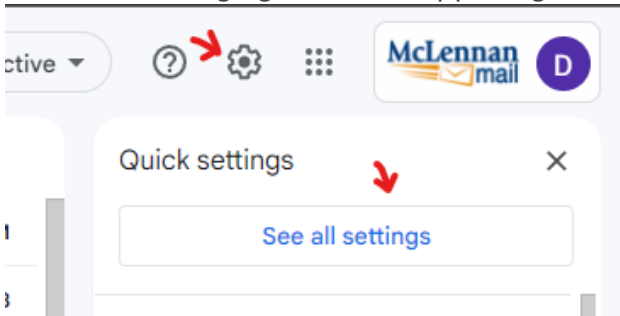
- [Gmail \(Computer, Android, iOS\)](#)
- [Mail \(iPhone\)](#)
- [Mail \(iPad\)](#)
- [Mail \(Mac\)](#)
- [Mail/Calendar \(Windows\)](#)

Your Student Email is Forwarding to a Personal Email

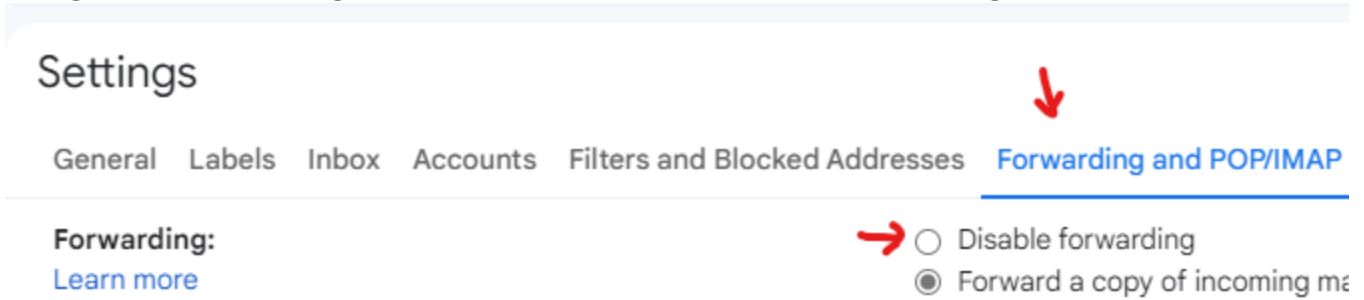
If you previously set up email forwarding, you can disable it using the following steps:

- Log in to your student email account: [Student Email](#)

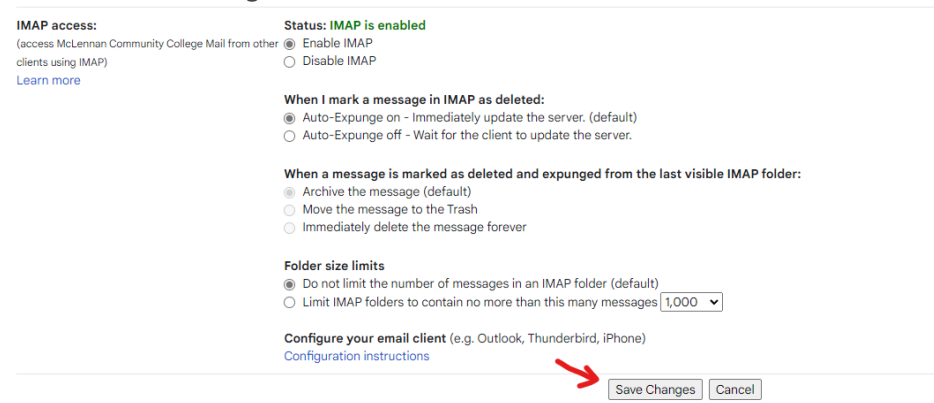
- Click the settings gear in the upper-right corner and select "See all settings."



- Navigate to "Forwarding and POP/IMAP" and select "Disable forwarding."



- Click "Save Changes" at the bottom of the screen.



Opt Out of MCC Emails

It is not possible to opt out of campus-wide emails such as newsletters, technical alerts, or general student announcements. These messages are sent directly to all active student email addresses.

Additional Details for Former Students

For students who have fully transitioned away from MCC, it is recommended to remove your student email from all devices and stop using it for any personal communications.

For additional details, see: [Students \(Google\) - Access Student Email: Termination of Email Access](#)

Sender Policy Framework (SPF)

Overview

There are times when emails may be blocked due to an issue with the email's domain. In this case, the SPAM filter will not automatically release these email(s). The email sender must correct the Sender Policy Framework (SPF), with their email domain, in order for the issue to be resolved. A detailed explanation of why these emails are blocked is outlined below.

Why are the emails blocked?

The McLennan Community College (MCC) Information Systems and Services (ISS) Infrastructure team has acted to raise our cybersecurity posture regarding incoming email messages. The first action is the filtering of email messages that fail Request for Comments (RFC) 7208 Sender Policy Framework (SPF). The second action taken is the filtering of email messages from domains with no published SPF record.

Initially, these messages will be quarantined. Quarantining the messages provides the MCC recipient the opportunity to review the affected message and release for delivery, if the MCC employee feels safe to do so. Additionally, quarantining the messages allows MCC employees and the ISS Infrastructure team to identify MCC partners and vendors that are not compliant with RFC 7208 and work with them to bring into compliance.

When MCC partners are identified to be out of compliance with RFC 7208, the ISS Infrastructure team will make every effort to assist the partner in configuring their email domain to be compliant. When outside vendors are identified to be out of compliance, by MCC staff, ISS Infrastructure members will provide our policy with the MCC staff member to share with non-complaint vendors and direct them to resources to assist them with becoming compliant.

Sender Policy Framework (SPF) Explained

We have come to a time and place where relaxed cybersecurity standards can have grave financial consequences for all. When a domain owner does not publish an SPF record, they leave their domain open for fraudulent use. Sometimes fraudulent emails are sent to their partners, changing money transfer details at the last minute, which redirect large sums of money into the accounts of the fraudsters. In this scenario both the sending and the receiving domain owners fall victim to the fraud.

Often, domain owners are unaware their domain name is being used fraudulently. When a domain's email identity is used fraudulently, or spoofed, the online reputation of that domain is

diminished. Typically, domain owners only become aware of the fraudulent use after their own legitimate emails are rejected by email domains, with SPAM filters in place, or where a large sum of money is unaccounted. At this time, system administrators are required to spend hours repairing their domain's online reputation, going through checks, to show the major email providers, they have eliminated the fraudulent use and their domain name may be removed from the list of fraudulent email senders. During this remediation period, conducting business for the organization becomes more difficult, due to the fact their emails are being rejected by most major email providers.

The Sender policy framework (SPF) was established as a tool for domain owners to guard against the fraudulent use of their domain name and protect their online reputation. When domain owners publish a properly formatted SPF record, they authoritatively declare the legitimate source(s) of emails sent from their domain. When an email passes a receiving domain's SPAM filter SPF checks, they know the email, from the sending domain, is safe to accept.

Last updated: 5/4/23