AHC Technology Council

October 1, 2025

Any Wi-Fi issues should be reported to ITS

Reviewing obsolescence standards for computers to make sure they stay current for security reasons. Need to identify computers that cannot upgrade to Windows 11.

Including Apple and Chrome.

The new standardized lectern will be about $6,000.

Reviewing the cost of the new K classroom chairs which are $800.

We were presented with the new policy on **Third-Party Applications and Microsoft 365 Accounts** which is attached.

The goal is to protect user data, endure compliance with security standards, and minimize the risk of data exposure from untrusted or over-privileged external applications.

While Microsoft 365 enables seamless integration with many applications, not all are appropriate for use in our college environment. AHC limits third-party application access to M365 accounts based on the entitlements (permissions) those applications request.

Many want access to your emails, your OneDrive or SharePoint files, Team chat data or messages, admin or organizational level permissions. Some have the ability to send emails on your behalf.

These apps will be blocked by default.

AHC allows integration with third-party applications only when the requested entitlements are limited to:

Basic Profile Information which includes your name, email address and user ID.

Calendar Assess to allow the app to view your availability and to book meetings and appointments for you.

Applications intended primarily for personal, non-work related use are not permitted.

If you frequently use third-party applications that request AHC blocked entitlements, you can still use the app by signing up directly with your@HancockCollege.edu email address rather than signing in through M365.

The policy lays out when and how to request an exception.

Respectfully submitted

Cary Gray 805-570-0620

CGray@HancockCollege.edu

Third-Party Applications and Microsoft 365 Accounts

Summary

This policy outlines the Hancock College IT department's position on integrating third-party enterprise applications with college-issued Microsoft 365 (M365) accounts. The goal is to protect user data, ensure compliance with security standards, and minimize the risk of data exposure from untrusted or over-privileged external applications.

Body

While Microsoft 365 enables seamless integration with many external applications, not all of these integrations are appropriate for use in our environment. Hancock College limits third-party application access to M365 accounts based on the entitlements (permissions) those applications request.

Allowed Application Permissions

We **allow** integration with third-party applications **only** when the requested entitlements are limited to:

- **Basic Profile Information:** This includes your name, email address, and user ID. These are used by applications to personalize your experience and confirm your identity.
- **Calendar Access:** This allows the app to view your availability and book meetings or appointments on your behalf.

These permissions represent a low level of risk and are essential for the function of many modern calendar and scheduling applications.

Blocked or Restricted Entitlements

All other permission scopes will be **blocked by default**, including but not limited to:

- Access to emails or email metadata
- Access to files stored in OneDrive or SharePoint
- Access to Teams chat data or messages
- Ability to send emails on your behalf
- Administrative or organizational-level permissions

Many third-party applications request more access than is necessary to function. Unfortunately, Microsoft allows developers to request any entitlements, and it is the vendor's responsibility to limit these to what is reasonably required. In many cases, this does **not** happen.

By granting excessive permissions, employees could unintentionally expose sensitive college data to **untrusted vendors**, increasing the risk of data leaks, compliance violations, and unauthorized data access.

Use of Applications for College-Related Work Only

Additionally, third-party applications integrated with Microsoft 365 accounts must be used strictly for Hancock College-related work activities. Applications intended primarily for personal, non-work-related use, or that do not have a clear connection to college business, are **not permitted** to link with M365 accounts. This restriction helps ensure that college resources and data are protected and used appropriately.

Alternatives for Accessing Applications

If you frequently use a third-party application that requests blocked entitlements, you can often still use the app by signing up directly with your **@hancockcollege.edu** email address rather than using the "Sign in with Microsoft" or M365 single sign-on option.

This method allows you to retain access to the application without granting it unnecessary access to your college M365 data.

Requesting an Exception

If you believe that an application requesting elevated M365 permissions is critical to your role or departmental operations, you may submit a software application installation service request to ITS for review. Please add in your request:

- The name of the application
- A justification for why these permissions are required for your work
- Any Hancock College approved alternatives considered

The ITS department will evaluate the security implications and business justification before granting or denying access.