Sinclair Community College

Working Remotely
A Guide for Faculty & Staff

March 2020

444 W. Third St, Dayton, Ohio 45402
www.Sinclair.Edu

Prepared By:
Dan O'Callaghan
Chief Information Security Officer
Daniel.OCallaghan@Sinclair.Edu

TABLE OF CONTENTS

Introduction

To support Sinclair employees when working remotely, this guide and the related links to resources within, cover the technology and information you need to create a successful and secure remote work environment.

In the event routine work or academic functions are disrupted due to prolonged campus or building closures, employees may find it necessary to teach classes or perform other work from off campus. Sinclair provides a variety of services and resources to remotely connect you with the College, colleagues, and students so that learning and the required support work can continue with minimal disruption.

These guidelines apply to full-time administrators, faculty, non-faculty professional and support staff working from alternate locations. These guidelines can also apply as needed to other categories of employees and contractors by Vice Presidents, Deans, and/or Directors.

Regardless of work location (at home or at a Sinclair site), employees need to:

- Be available and accessible during their working hours
- Be responsive to meeting college, department, and supervisor needs related to maintaining operations for student education
- Maintain appropriate confidentiality of college work, including but not limited to student education records
- Retain college records, including records created while working remotely, in a secure fashion and in accordance with existing applicable records retention schedules and policies
- Exhibit a spirit of teamwork and flexibility to meet college (student) needs during this emergency

Working from alternate locations and schedules will be coordinated and controlled by supervisors in concert with the student completion and in-person service plans of the Vice Presidents, Deans, and Directors.

This policy may be revoked or altered at any time that the supervisor believes that the quality of support is suffering, if departmental needs change, or if there is an immediate need to return to your primary location and/or work schedule.

The typical workday for an employee working from an alternative location will be 8:00 AM to 5:00 PM Monday through Friday, excluding holidays, which are already part of the college calendar, or other scheduled hours the employee has been previously approved to work. Employees should continue to submit vacation time, personal time, and sick time according to policy. Other hours may be approved by the supervisor to work as part of the alternative working arrangement. Regardless of work location, all work hours for non-exempt (hourly) employees must be tracked. All part-time employees are expected to remain within the 28 hour maximum work week unless otherwise directed by management.

Employees must be available by phone and email during their scheduled work hours. Sinclair will inform employees if they need to start reporting their hours worked.

Employees may be assigned alternative work duties, including but not limited to computer-based, remote professional development activities, web-based research on higher education or operational innovations, or assigned professional reading.

Sinclair will make reasonable efforts to ensure that employees have the necessary computer equipment and software (college-issued or individually owned) to complete assigned work; however, employees are responsible for providing their own adequate internet access. Employees who have already been provided with college-owned computers, laptops, iPads, or cell phone, will be expected to use that equipment.

Security, Privacy, and Compliance

Remote work does **not** relieve the College and employees from the ethical, moral, and legal responsibilities related to protecting student records, personal information, and other sensitive data. All College policies related to security, privacy, and compliance still apply. The flexibility of working remotely inherently involves real cybersecurity risks. With increased remote work, there is increased risk of employees accessing data through unsecured and unsafe Wi-Fi networks, using insecure personal devices to perform work, and not following general security protocols. The guidelines and technologies described in this document are currently **the only approved and vetted methods** for accessing and using Sinclair technical resources. Any employee seeking to use other methods must first obtain documented approval from Sinclair's CISO/College Administration.

Key excerpts from Sinclair's Acceptable Use of Information Technology Policy:

(https://it.sinclair.edu/index.cfm/services/student-and-guests-services/policies-and-security-information/acceptable-use-of-information-technology-policy/)

- Users processing, accessing, or transmitting personal information must adhere to effective practices designed to minimize risk of compromise, to safeguard the information, and use it only in accordance with College policy and within the scope of their duties. Personal information is defined as first name (or initial) and surname, in combination with any of the following:
  - Social Security Number
  - Driver's license number or state identification card number
  - Financial account, debit card, or credit card number(s)
  - Other information that creates a 'material risk of the commission of the offense of identity fraud or other fraud to the individual.'
- Users processing, accessing, or transmitting data containing student record information must comply with Family Educational Rights and Privacy Act (FERPA) guidelines. All student information must be treated as confidential, even public or "directory information" may be subject to restriction.
- Users must ensure appropriate and effective security methods are used when storing— downloading, recording, entering, or otherwise saving—personal information or other sensitive information, particularly on non-central storage devices or locations. Personal information on mobile devices, including but not limited to, laptops, tablets, smartphones, PDAs, and any wireless telecommunication devices, must employ a College-approved technical security method.
- Personal information may not be stored on mobile devices or on other removable storage media, including, but not limited to, diskettes, CDs, memory sticks, USB drives, and personal "Cloud" storage services, unless the information is protected from theft and other methods of unauthorized access using encryption or similar technology approved by the Information Security Office.
- Users should report any incident of compromise or suspected compromise of any Sinclair information asset to the IT Help Desk, the Information Security Officer, or the CIO as soon as possible.

Sinclair Community College considers any violation of this policy as a serious offense. Violators are subject to College disciplinary action as prescribed in conduct policies, the student handbook, employee handbooks, and other applicable College policies and standards.

Basic Technology Required

This section covers the basic technical equipment and access most Sinclair employees can use to work remotely. The vast majority of employees need only the top two—a computer and an Internet connection. Certain jobs may require specialized hardware, software, or access. If you believe you need additional or specialized technology, consult with your supervisor.

- **Laptop or desktop computer** with a supported operating system (OS) and all current updates (Enable auto-update is recommended). Recommended OS is Windows 10 or macOS X (macOS 10.7 or later). Integrated OS security software (such as Windows Defender/Firewall) *must be enabled and updated*. Employees technically adept with Linux may use a current version, but the College does not offer support for Linux-related issues. NOTE: Tablet/mobile devices *may* also be supported but are likely limited in flexibility and rely extensively on the individual's comfort and expertise using them.
- **Internet Connection –** A "Broadband" Internet connection is required. This may be via a commercial ISP (e.g., Xfinity, AT&T, Cincinnati Bell, etc.), or via a mobile access "hotspot" provided by a cellular service provider (e.g. Verizon, AT&T, Sprint, T-Mobile, etc). A *minimum* bandwidth speed of 3 Mbps up/down is required. Faster connections are required for video, streaming, and other more memory intense applications.
- **Microphone and speakers** (optional, but highly recommended for live conferencing/teaching) **–** these may be integrated in the computer or monitor. An alternative is to use an external microphone and computer speakers. Highly recommended is a noise-cancelling Bluetooth or USB headset. If you are purchasing a speakerphone/microphone device, it is strongly recommended to follow suggestions on the Zoom support site: https://support.zoom.us/hc/en-us/articles/201362023-System-Requirements-for-PC-Mac-and-Linux#usb.
- **Webcam** (optional unless video conferencing/teaching is required) **–** A camera may also be integrated into the computer or monitor. Similar to the microphone/speaker options, you can also use an external USB camera for video conferencing. If you are looking to purchase a camera, it is strongly recommended to follow suggestions on the Zoom support site: https://support.zoom.us/hc/en-us/articles/201362023-System-Requirements-for-PC-Mac-and-Linux#usb.
- **Cell Phone** (may be optional, depending on role) – Sinclair's Mitel solution provides the ability to forward your office phone to your cellphone (see details in this guide). Consult with your supervisor to ensure forwarding your calls is required and/or appropriate.

Prepare and test your technical environment in advance! It is best to know and test which options will work for you before you actually need them. Test access to your equipment and resources at home before the need arises. If you have questions or issues, contact Sinclair's IT Help Desk at 937-512-4357. If you do not have equipment at home that meets the above standards, please consult with your supervisor.

Forwarding Your Telephone

Important! You can change your availability state from off-campus in order to transfer your calls, *but you must first follow the steps below while on campus* to initially configure the forwarded phone number. After the initial setup, you can forward your calls remotely using the voicemail system to change your availability state (see below)

Step 1—Configure the "Custom" State option

From your on-campus desk phone, configure the phone number you want to transfer to:

1. Press the **Options** button
2. Enter your voicemail password and press **OK**
3. Press the **right arrow** button, then **down arrow** to "Custom"
4. Press the **Edit** button
5. "Forward Calls" can be set to Always or No Answer (press the **right arrow** button to change)
6. Arrow down to "Always dest" and enter the destination number for your calls (including the area code)
7. "Simulring" should be set to "Off" to ring your destination number only
8. Press the **Back** button, **OK,** and **Exit**

Your Custom state is now configured to forward calls to the alternate phone number of your choice and ***your availability state is set to Custom***. You can change your state between Available (in the office) and Custom (forwarded to your alternate number) by either of the methods below:

Step 2 – Change your Availability State

From your desk phone:

1. Press the **State** button
2. **Arrow** to either Available (in office) or Custom (forward to alternate number)
3. Press the **OK** button

From the Voicemail system:

1. Dial 937-512-5400
2. Press **#** to enter the voicemail system
3. Enter your extension number
4. Enter your password and press **#**
5. Press **7** to change mailbox options
6. Press **2** to configure availability state
7. Press **5** to set Custom (forward to alternate number)

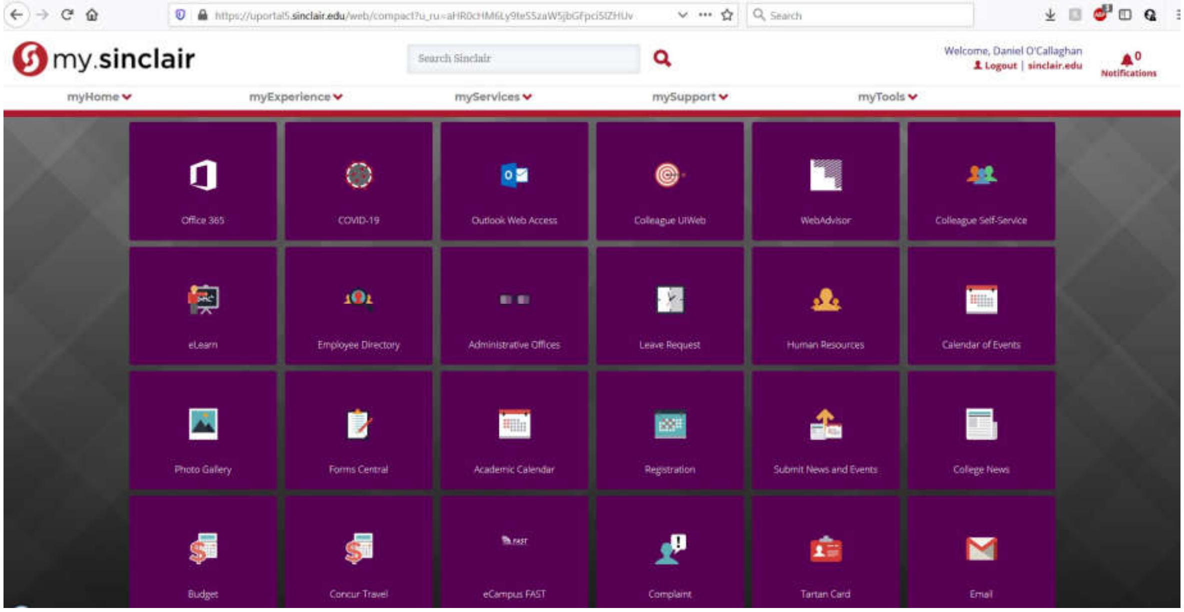
NOTE: The help desk can also set up and/or change your availability states when you are away from your office. Please call 937-512-4357 for assistance.

Accessing Sinclair Resources – My.Sinclair.edu

Sinclair's Web Portal "my Sinclair" (https://my.sinclair.edu) is the primary digital gateway to Sinclair. Login with your Sinclair credentials from any device with an Internet connection. While any browser will likely connect, Sinclair websites are optimized for the following web browsers: Google Chrome, Firefox, and Safari (Mac). Please use one of these browsers for the best experience.

The apps or "portlets" in MySinclair provide access to all of the applications and services the majority of Sinclair faculty and staff need, and should be the first place to login when working remotely.

NOTE: Colleague UI is now accessible via My.Sinclair. You DO NOT NEED to use App Depot to access.



Some of the portlets available via mySinclair:

Academic calendar
Academic catalog
Administrative offices
Advising appointment
Alumni
Booklist
Budget
Budgettransfer
Bursar
Colleague Change Request
Colleague-UI Web
College calendar
Concur
Course planning
Covid19 preparedness
Course schedule
Curriculum management
Dawn portal

Directory - employee
Disabilityservices
Elearn courses
Elearn training support
Enrollment-center
Facility-work-request
Faculty assignments
Faculty-staff news
Financial-aid
Forms central
Help-desk
HR news
Human Resources
Informer
Info-tech
Jira
Leave request
Library

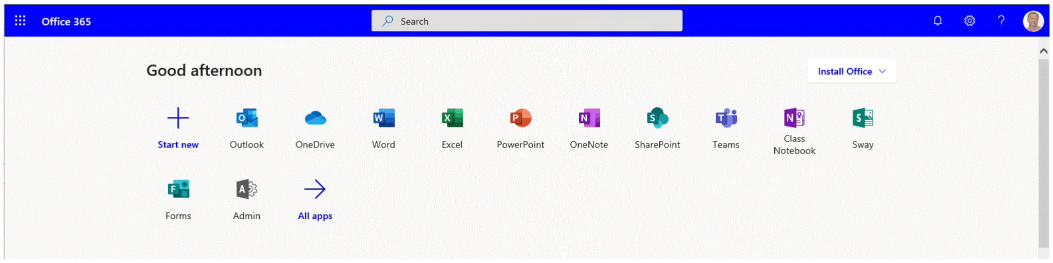
Mobile app
MS imagine
New-student-orientation
Nontuition payments
Office 365
Off-campus-file-access
Payroll
Photo-gallery
Planned-downtime-calendar
Print-on demand
RSR
Search-google
Secureupload
Selfservice (Colleague)
SHS upload
Sinclair IT
Software-request
Spamfilter (mimecast)

Student-behavior
Studentfinance
Student records
Student refunds
Student-success-plan
Submit-news-events
Testingcenter
Test-management-system
Title IX
Topnews
Traffic alert
Transcript-request
Transfer equiv
Tutorial-services
WebAdvisor (Colleague)
Web crd
Web mail
Zoom

Accessing Sinclair Resources – Office 365 and One Drive

Office 365 is Microsoft's online "cloud" portal for email, data storage, productivity apps, and collaboration tools. Sinclair provides access to Office 365 for all faculty and staff, and will soon provide access for all students. Office 365 is accessible 24x7x365, on any device, from anywhere in the world. Since Sinclair has a contract/license for O365, employees can use these "cloud" resources as if they are "on the network"

To access O365, visit https://www.office.com/ and sign in with your Sinclair network credentials to access OneDrive, Word, Excel, Outlook, OneNote, PowerPoint, and more…

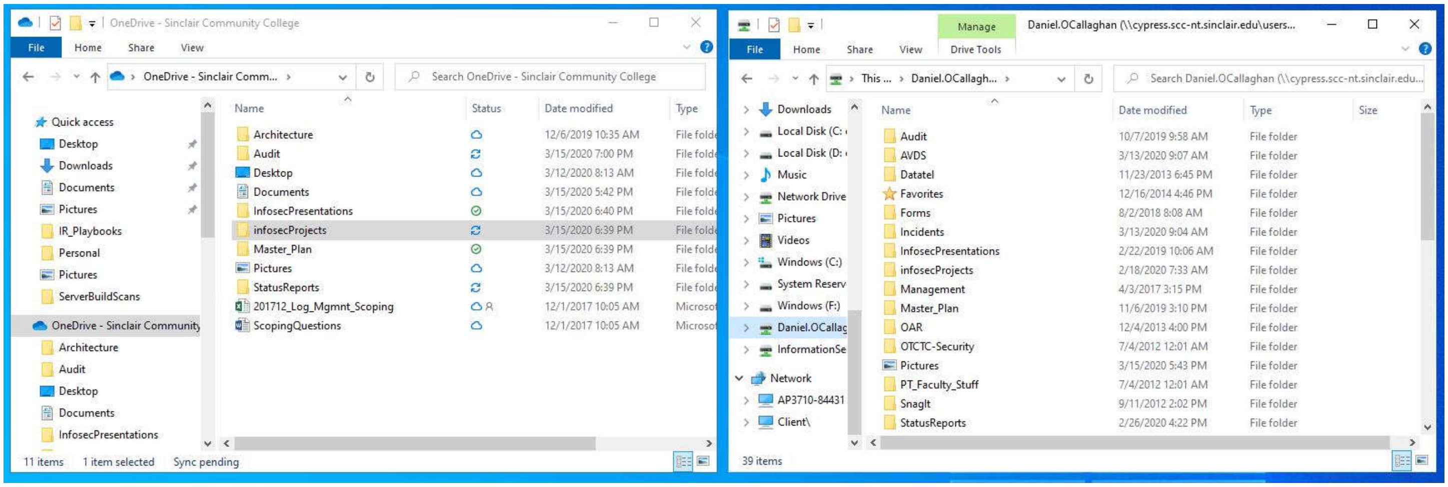


One Drive

One of the most useful O365 features is "OneDrive". A simple analogy is to consider One Drive as your cloud-hosted "H-Drive". Files you normally access from Sinclair H-Drives or Department file shares can be safely stored, shared, and synced to/from OneDrive. Basic instructions for using One Drive can be found here: https://support.microsoft.com/en-us/help/17184/windows-10-onedrive

Syncing files and folders from your campus PC and network shares to OneDrive will create duplicates of the files in both OneDrive and on Sinclair's network, and keep them "in sync". This will permit you to securely access them remotely. To begin syncing folders, open two instances of Windows Explorer.

To do this, open File Explorer (Windows Explorer in Win7) once by clicking its launch icon, then right-click the icon and select **File Explorer** again from the pop-up menu to open a second instance; arrange them so you can see both. In one instance, navigate to the One Drive cloud icon. In the other, navigate to the folder you want to synch. To begin syncing, simply select the folder you want to sync and drag it to the cloud icon. *NOTE: IT recommends syncing individual files/folders within your "H-Drive" or other network share, not the entire share folder. Users have reported issues when attempting to sync the entire network share folder.*



Name	Status	Date modified	Type
Architecture	☁	12/6/2019 10:35 AM	File folde
Audit	⟳	3/15/2020 7:00 PM	File folde
Desktop	☁	3/12/2020 8:13 AM	File folde
Documents	☁	3/15/2020 5:42 PM	File folde
InfosecPresentations	✓	3/15/2020 6:40 PM	File folde
infosecProjects	⟳	3/15/2020 6:39 PM	File folde
Master_Plan	✓	3/15/2020 6:39 PM	File folde
Pictures	☁	3/12/2020 8:13 AM	File folde
StatusReports	⟳	3/15/2020 6:39 PM	File folde
201712_Log_Mgmnt_Scoping	☁	12/1/2017 10:05 AM	Microsof
ScopingQuestions	☁	12/1/2017 10:05 AM	Microsof

11 items 1 item selected Sync pending

Name	Date modified	Type	Size
Audit	10/7/2019 9:58 AM	File folder	
AVDS	3/13/2020 9:07 AM	File folder	
Datatel	11/23/2013 6:45 PM	File folder	
Favorites	12/16/2014 4:46 PM	File folder	
Forms	8/2/2018 8:08 AM	File folder	
Incidents	3/13/2020 9:04 AM	File folder	
InfosecPresentations	2/22/2019 10:06 AM	File folder	
infosecProjects	2/18/2020 7:33 AM	File folder	
Management	4/3/2017 3:15 PM	File folder	
Master_Plan	11/6/2019 3:10 PM	File folder	
OAR	12/4/2013 4:00 PM	File folder	
OTCTC-Security	7/4/2012 12:01 AM	File folder	
Pictures	3/15/2020 5:43 PM	File folder	
PT_Faculty_Stuff	7/4/2012 12:01 AM	File folder	
SnagIt	9/11/2012 2:02 PM	File folder	
StatusReports	2/26/2020 4:22 PM	File folder	

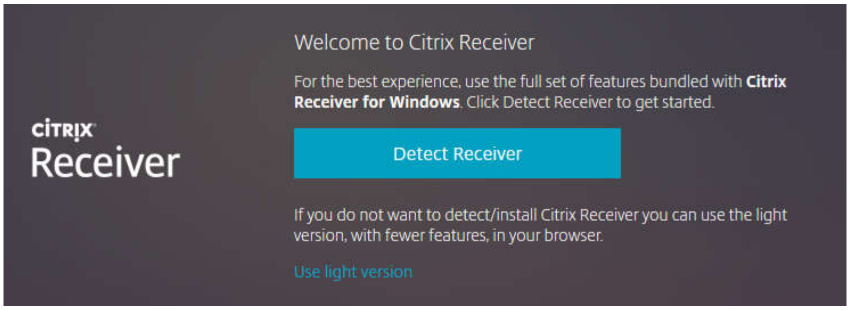
39 items

Accessing Sinclair Resources – App Depot

The App Depot system can be used on computers with Windows or macOS operating systems.[1]

Using App Depot for the first time.

1. To access App Depot, open a web browser and go to **appdepot.sinclair.edu**.
2. Login with your Sinclair network username and password.
3. If you are using an HTML5-capable browser (like Chrome), click on the **Use light version** link, and skip to step 6.

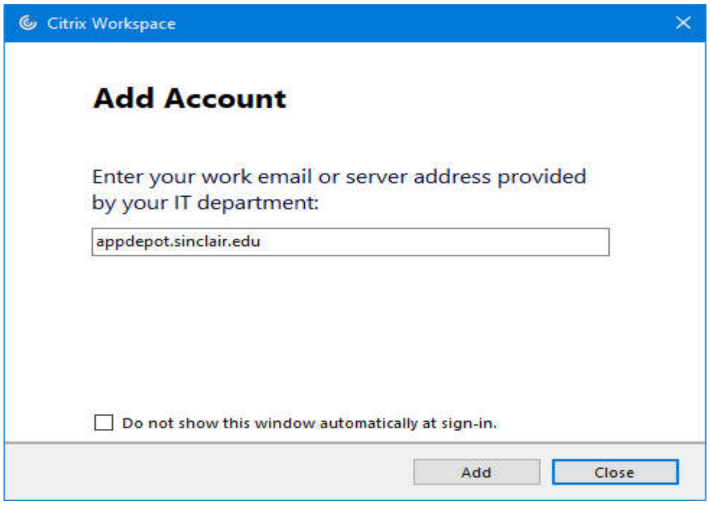


Welcome to Citrix Receiver

For the best experience, use the full set of features bundled with **Citrix Receiver for Windows**. Click Detect Receiver to get started.

If you do not want to detect/install Citrix Receiver you can use the light version, with fewer features, in your browser.

4. If your browser is not capable of using the light version of Receiver, and you are on a Windows PC, open the Microsoft Store application on your Start menu. Search for the “Citrix Workspace” app. Install this application on your PC. After the installation finishes, launch it from either the Microsoft Store button or the Start menu. (The Citrix Workspace app is also available in the app store on macOS, similar instructions apply)
5. Once the Citrix Workspace app launches, you will be asked to enter your work email or server address. Enter “appdepot.sinclair.edu” and click the Add button.



Add Account

Enter your work email or server address provided by your IT department:

appdepot.sinclair.edu

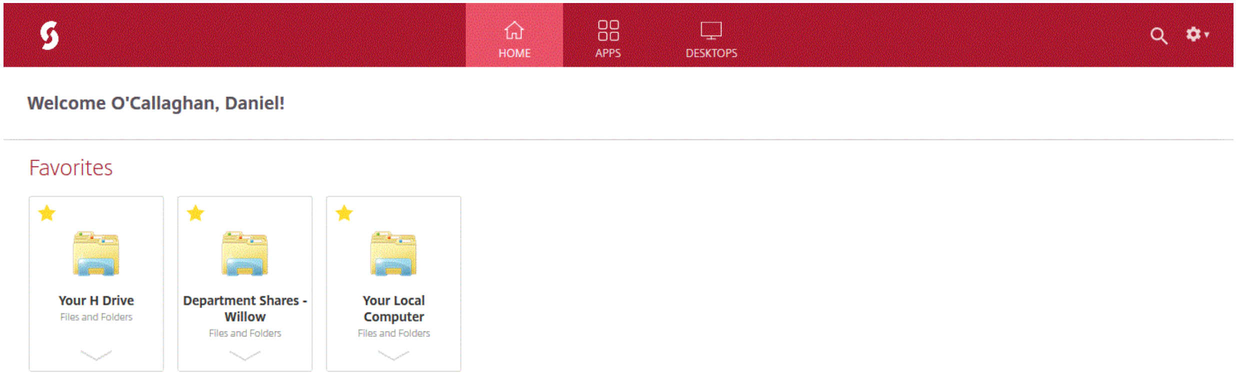
□ Do not show this window automatically at sign-in.

6. You will be prompted to enter your user name and password. **Use your Sinclair network credentials**.
7. When App Depot opens, you will likely default to the HOME tab at the top of the window. You should also see the APPS and the DESKTOPS tabs.

Linux, iOS and Android devices are also supported, but they are not covered in these instructions.

App Depot – The HOME Tab

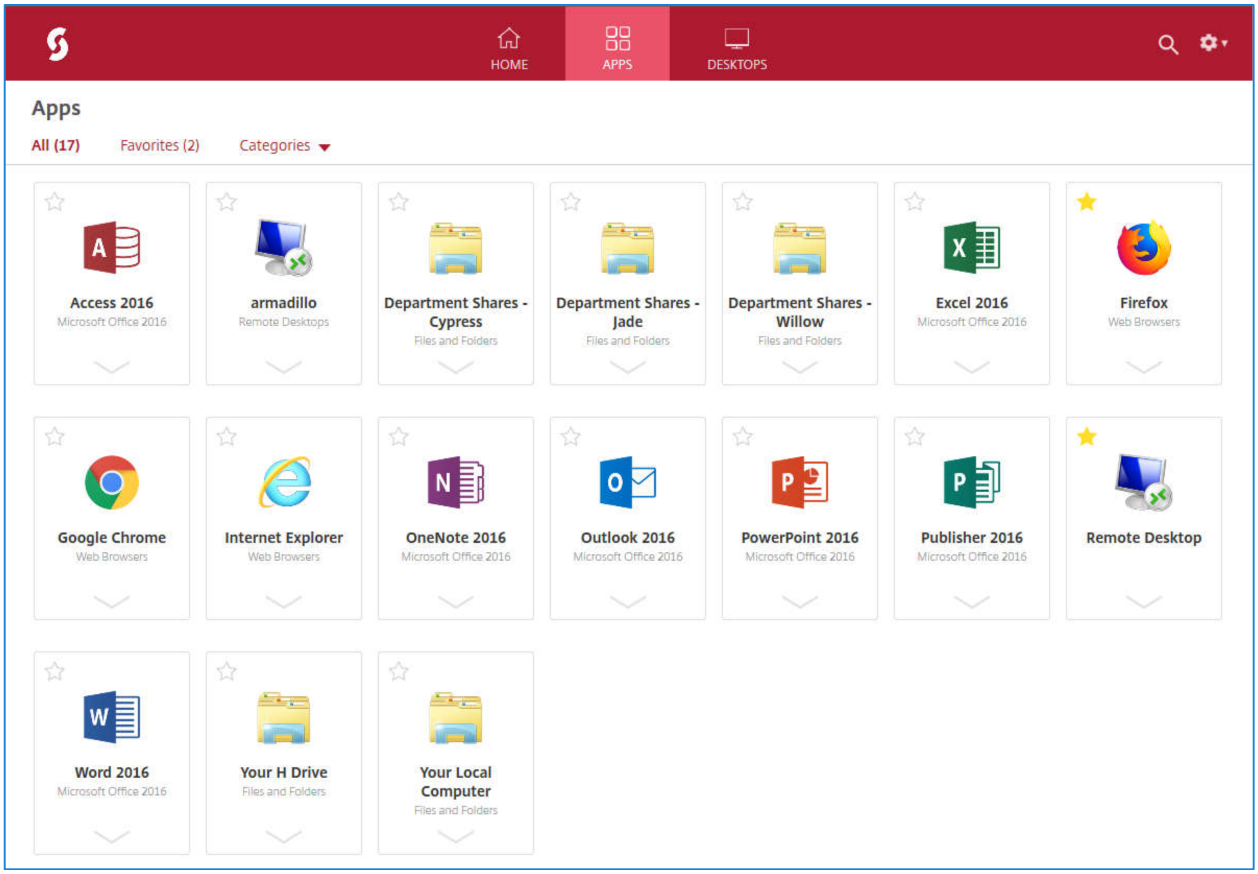
1. The HOME Tab is the default landing page after logging in. From the HOME tab, you will see and can access any apps you have "starred" as a favorite in the APPS or DESKTOPS tabs.



Welcome O'Callaghan, Daniel!

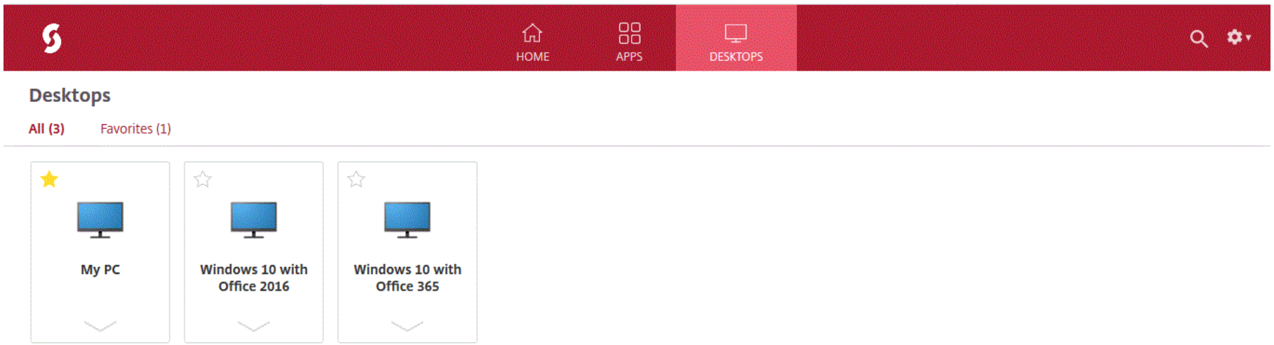
App Depot – The APPS Tab

1. From the Apps tab, you can access your local computer (the computer you are using, not your on-campus PC), your H: drive, your shared drives, Microsoft Office applications, and web browsers. You may also have other applications assigned to you, depending on your role in the college. If you click the star next to any application, it will be added to your Favorites and will be accessible from the HOME tab when you log on



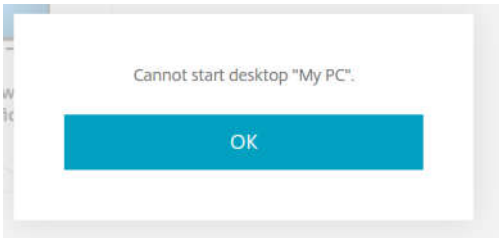
App Depot – The DESKTOPS Tab

1. From the DESKTOPS tab, you can access "virtual" desktops and operations systems. If specifically authorized, you may also have access to the "MY PC" Desktop, which provides remote access to your Sinclair on-campus PC. If you click the star next to any application, it will be added to your Favorites and will be accessible from the HOME tab when you log on



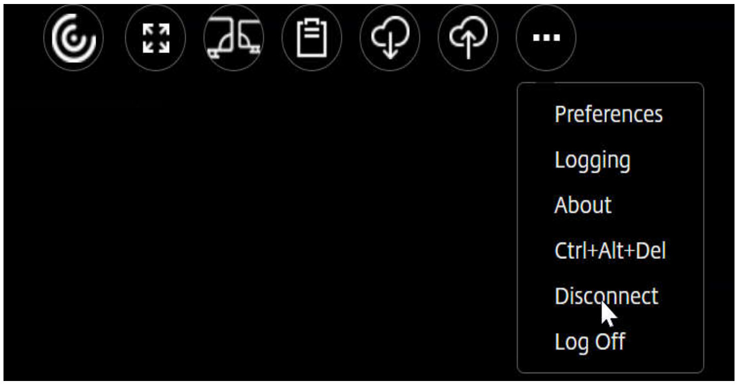
My PC (PC Connect—ONLY for Windows PCs)

2. Before you can connect to your on campus PC, you will need to request and configure this from on-campus. You will need your PC Name (obtain this by typing "PC name" in the search bar on your desktop) and your Tartan ID number. Call the Help Desk at 4357 and let them know you need remote access to your on campus PC. The Help Desk Analyst will assist with this process. After approval and setup, your on-campus PC will be accessible via the App Depot DESKTOPS tab.
3. When you click the "My PC" icon, if your on-campus PC is not awake, you may get this message:



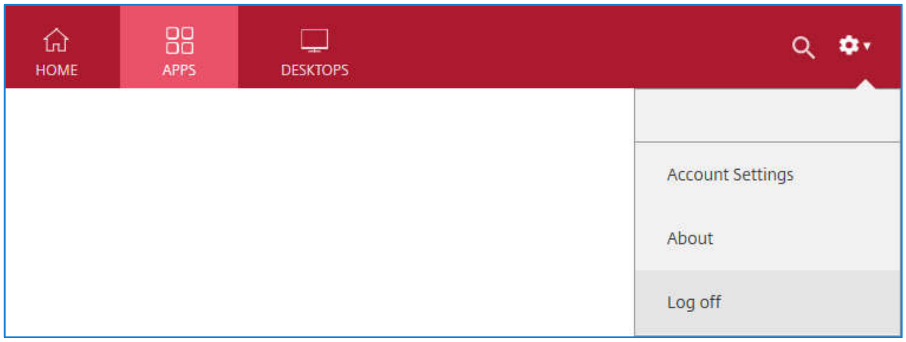
Cannot start desktop "My PC".

4. Click OK, wait several minutes, and try again. By then, your PC should be awake, and you should have access to your desktop.
5. When finished using your on-campus PC, it is important to click the three lines at the top of your screen, and then click the "…" button and choose Disconnect.



App Depot – Logging Out

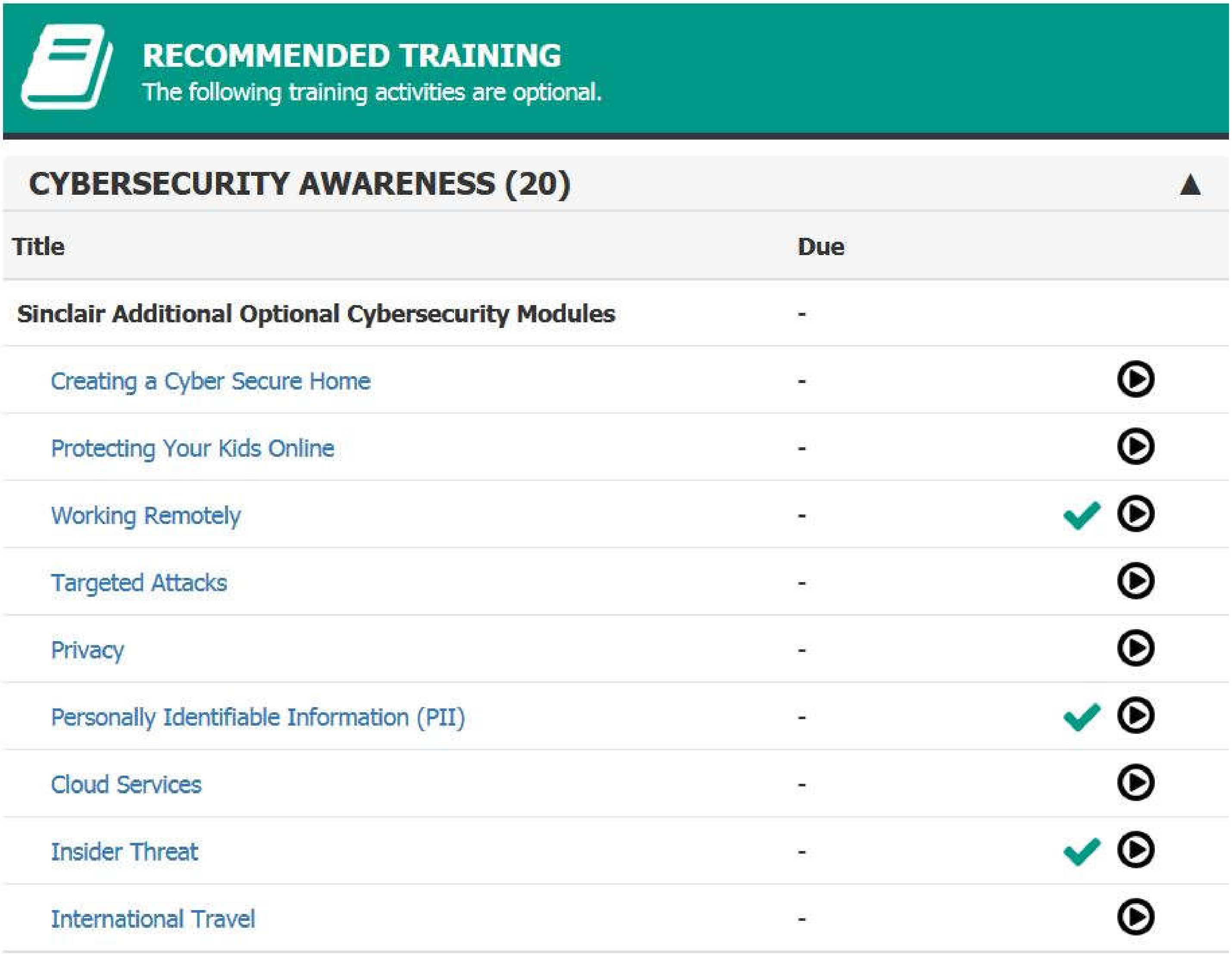
1. When you are finished using App Depot, both for securely closing the connection and to free up the license for use, it is important to close any open app windows and to log off.



For questions or additional information, contact the IT Help Desk at 937-512-4357 or at helpdesk@sinclair.edu.

Additional Security Awareness Training

While all Sinclair employees complete basic Security Awareness training during onboarding, it is strongly recommended to complete additional training modules specifically related to working remotely. These may be accessed by logging in to **https://access.sans.org**, under the “**Sinclair Optional Cybersecurity Modules”**. The “Creating a Cyber Secure Home” and “Working Remotely” modules are highly recommended.



RECOMMENDED TRAINING

The following training activities are optional.

CYBERSECURITY AWARENESS (20) ▲

Title	Due	
Sinclair Additional Optional Cybersecurity Modules	-	
Creating a Cyber Secure Home	-	▶
Protecting Your Kids Online	-	▶
Working Remotely	-	✓ ▶
Targeted Attacks	-	▶
Privacy	-	▶
Personally Identifiable Information (PII)	-	✓ ▶
Cloud Services	-	▶
Insider Threat	-	✓ ▶
International Travel	-	▶

A “fact sheet” highlighting important basic concepts for working remotely: https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-WorkingFromHome-FactSheet.pdf