Working and Teaching from Home
Best Practices

Information Technology Services

Make sure your laptop is ready

If you have a university-owned laptop, make sure your Operating System has the latest software updates from Microsoft or Apple and has the most current anti-virus and anti-malware (West Georgia uses Ivanti Antivirus) installed. The best way to do this is to plug your laptop into the campus network's wired connection from your office and leave it overnight. This will allow our automated services to deliver and execute all needed updates. Also, make sure you have all of the cables you need to power the laptop at home.

Make sure files are accessible

Make sure any electronic files you need are accessible. Based on your typical workday, think about the files you use regularly and be sure you will have access to them remotely. You can move all files that don't have confidential or sensitive data (see definitions below) to your Google Drive. If you are teaching, you can store files in CourseDen. Files containing confidential or sensitive data can be stored on an encrypted portable drive (such as a Kingston IronKey, which is available from SCW), or on the university network's file share. Make sure you can access your network share from home using the WiredEQ VPN.

Using personally-owned devices

If you are using a personally owned computer while working from home, it should be current on software updates and have current antivirus/anti-malware software installed. If you are using a PC with Windows, you can set your computer to update automatically, and we recommend using Windows Defender for Antivirus.

If you are using a Mac, you can ensure you are patched and up-to-date automatically.

Make sure your computer has the latest software updates and the most current anti-virus/malware installed.

Virtual Meetings, Collaboration, and Classrooms

UWG provides access to several tools to facilitate meetings online. It’s important to discuss the meeting and collaboration tool(s) you want to use with your coworkers and students. All employees have access to Microsoft Skype and Google Hangouts. Faculty can use the tools in CourseDen (Collaborate Ultra) to set up virtual classrooms:

- Use of Google Hangouts for Individual and Group Chat, Easy Launch of Video calls.
- Use of Google Meet for Video Meetings: Google is providing free access to advanced Google Meet features until July 1, 2020. This version supports up to 250 participants, live streaming and recording.

Refer to Google's G Suite Learning Support Center on Hangouts Meet Training and Help for more information.

Please note: full support is available for Collaborate Ultra and Kaltura, and Google Meet/Hangouts and Microsoft Skype support is currently ITS’s best effort.

Updating your office voicemail

If you use the phone in your office as part of your routine tasks and plan to work from home, we recommend you change your outgoing greeting to say "I'm currently working from home. If you need to speak with me please email me at jdoe@westga.edu with your message and a way to contact you. I will reach out as soon as I am able".

See the Voicemail Guide for instructions on how to set up your voicemail messaging.

Do I need to use VPN?

You should first attempt to work from home without using the VPN and Remote Desktop until you determine if you need to use either.

Many tasks we perform every day can be done without using the VPN:

- Email using Gmail
- Collaboration tools - Google groups, Google Drive, Google Docs, Google Sheets, Google Hangouts, Google Chat
- CourseDen
- BanWeb
- PeopleSoft Self Service
- OneUSGConnect for time sheets, viewing pay stubs, etc.
- DevelopWest
- Office 365

General VPN Access

Personal Devices and State-Owned Devices

Personally owned devices must be up-to-date on both OS patches and anti-virus/anti-malware software.

1. If you use Banner 9 Admin Pages or PeopleSoft Financials you'll need the access VPN, which is available for personally owned devices as well as state owned devices. VPN Instruction [PDF]
2. Argos Reporting and Banner eXtender also require the use of the access VPN.
3. If you're using a personal device and you need to connect to the desktop computer in your office, you can set up remote desktop. The remote desktop connection will allow you to connect to and use your desktop computer from your home computer. If you use Remote Desktop, you will not need Wired Equivalency (see below). Remote Desktop Instructions [PDF] or [Remote Desktop Video Tutorial]

Wired Equivalency

State-Owned Devices ONLY

Due to restricted access and the sensitive nature of the data, there are some applications which require the use of a state owned device and a separate VPN.

1. OneUSGConnect for HR staff.
2. Access to the file shares (Y: Drive, etc). You can also use Remote Desktop.
3. Some PeopleSoft Financials functions.

Video Tutorials

- Remote Desktop Connection (2:26)
- VPN with Remote Desktop Setup (4:57)
- VPN Install/Setup (3:36)

Data Definitions from ITS Handbook

1. Confidential data: Data for which restrictions on the accessibility and dissemination of information are in effect. This includes information whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

2. Sensitive data: Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration or destruction will cause perceivable damage to the participant organization. Example: personally identifiable information, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) data, or data exempt from the Georgia Open Records Act. (Source: SP 800-53 Rev. 4)

3. Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. (Source: OMB Memorandum M-07-1616) Information which can be used to distinguish or trace the identity of an individual (e.g., name, Social Security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). (Source: SP 800-53 Rev. 4) Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (source: OMB Circular A-130)