**Telecommuting Guide for SPHHS Move**

**Faculty and staff are encouraged to telecommute during the move period. Please refer to these tips before and during telecommuting.**

* Communicate in advance with your supervisor about the expectations for your work while you are telecommuting and agree on specific deliverables.
* Check your calendar and reschedule any meetings that need to be conducted in-person. If necessary, inform internal and external customers of your limited accessibility during the move.
* Evaluate upcoming deadlines that may be impacted by working remotely. Keep that into account also when setting new commitments.
* Discuss with your supervisor in advance the preferred or required methods of communication and accessibility – email, phone, IM etc.
* Keep your cell phone charged and accessible to you during work hours. Make sure your cell phone has a signal.
* Make sure you and your supervisor have each other’s cell phone numbers, as well as numbers for other crucial staff you typically contact.
* Check your work voicemail regularly by dialing 202-994-2000 and following the directions.
* Regularly check your email and promptly respond to urgent messages.
* If you are using a laptop for work, keep it accessible and charged. If you are working outside of your home, make sure to bring an adapter. Secure all university-owned computers and other portable electronic devices by employing strong passwords and physical protections.
* Use only secure password-protected Wi-Fi connections. Do not use public Wi-Fi connections.
* Designate work space that would provide a productive and quiet working environment.
* Have a family preparedness plan to ensure that childcare and other relevant arrangements are in place.
* Take breaks from work. In particular, make sure to take at least a 30-minute meal break.
* For non-exempt staff: continue to clock in/out; if unable, make a record of your work time and overtime (follow the pre-approval procedure for overtime, as usual).
* Do **not** take outside of the university hard copies of any documents that contain confidential information.  At all times, make sure to keep confidential information secure.
* Work with the IT department to establish a VPN access, if needed. Refer to the *Access Network Drives from Home* instructions that were distributed by IT.
* Utilize Google Chat to communicate with your supervisor and co-workers as an alternative.
* Utilize share-drives, Dropbox or Google Drive to collaborate with other staff on documents.
* Access confidential information at the source. Any files that contain confidential data should **not** be kept on local PCs, CDs, DVDs, external hard drives, USB flash drives, etc.  These files should be stored in a secured network folder that is only accessible by authorized personnel.  Email is inherently insecure and confidential data should never be sent via email unless encryption software is used.
* Additional resources and training on data security is available here: <http://it.gwu.edu/resources>
* Refer to these policies related to telecommuting: <http://hr.gwu.edu/policies-related-telecommuting>