UNIVERSITY OF PUGET SOUND
TELECOMMUTING TERMS AND CONDITIONS
March 2020

General Terms and Conditions

1. I understand telecommuting is a mutually agreed upon work alternative between me and the University of Puget Sound, as indicated by my supervisor's approval, for the benefit of the University. I understand that the university may modify or end my remote work arrangement at any time.

2. I agree to participate in any telecommuting training and evaluation activities required and/or recommended by my supervisor.

3. I agree to keep my supervisor informed of my progress on assignments worked on at home, including any problems which I may experience. My supervisor and I have agreed upon a work planning/monitoring process for my telecommuting day(s).

4. I agree to structure my time to ensure my attendance (either in person or via video/audio conferencing) at required meetings and University of Puget Sound events as designated by my supervisor.

5. I understand and accept the special responsibility I have as a telecommuter to facilitate communication with my colleagues and stakeholders I serve. I agree to stay connected and current on departmental and other matters applicable to my work.

6. I understand that any University equipment I use at home must be protected against damage and unauthorized use, that equipment owned or provided by the University will be serviced and maintained by the University, that access to University equipment at my home must be granted to appropriate officials, and that equipment I provide will be at no cost to the University and will be maintained by me.

7. I understand that the University will not be responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of my residence.

8. I agree to maintain my home work space with appropriate ergonomic and safety considerations, with adequate lighting and ventilation, and free from distractions.

9. I understand that I must safeguard and protect records from unauthorized disclosure or damage and that all records are the property of and must be returned to the University.

Technology and Security Terms and Conditions

10. Where possible, a university issued computer should be used to process university-related work. If not possible, ensure that no university data is stored on your local, personal machine. Instead, take advantage of the university's shared drives or Google Drives.

11. Virtual Private Networking or VPN should be used at all times while working within university systems including but not limited to my.pugetsound.edu or canvas.pugetsound.edu. More information about the university's VPN can be found at https://www.pugetsound.edu/about/offices-services/technology-services/help-support/self-help/vpn/

12. Any time a university computer is being operated on a public wireless network, the VPN must be used.

13. University laptops should never be left unattended in a public place or left in a place in which they could be easily stolen such as plainly visible inside a locked car.

14. When leaving a university computer system, regardless of location, it should be left in a locked password-protected state so as not to allow others to access it without your knowledge.

15. As always, your password should never be shared with anyone.

16. The university's computer is intended for use only by the person to whom it was issued. It should not be used as a family computer system, nor should it be shared with others.

17. Antivirus and Operating Systems updates are configured to automatically update. Do not alter this configuration. If you are using a personal computer for university work, it must have an approved antivirus software that is configured to automatically download current updates. The Operating System must be up to date and configured to download updates and patches automatically.

18. If using a personal, wireless network in a residence, the wireless network should be configured with at least WPA2 protection, an SSID name that is not the default from the manufacturer, and a username/password combination that is not the manufacturer's default. Tips on properly securing your wireless router can be found here: https://support.microsoft.com/en-us/help/17137/windows-setting-up-wireless-network