Remote Work Guidelines
University of Maine System
COVID-19 Response

Purpose

University Services Human Resources is providing updated remote work guidelines to assist campuses during this time of pandemic.

Eligibility

Remote work is available to employees who:

- Have work responsibilities that can be performed at home without adversely affecting quality, productivity, and the needs of the University, and
- Have ongoing access to telephone, adequate computer resources and Internet at home.

Employees may request to work remote. Management has sole authority to approve or deny requests, although during this time we ask that a flexible approach is taken to these requests. If a request is denied, the employee may ask for review by the university Human Resources office, which will attempt to help develop a resolution acceptable to both the supervisor and the employee.

Criteria

Remote work is not suitable or practical for all work or all positions. If an employee has the proper technology and has work that may be completed from home, we encourage managers to consider the request.

Conditions

1. We recommend the following provisions:

    a. Expectations about work to be performed from home and regularly scheduled check-in times or meetings.

    b. Core hours when the employee will be available to supervisors, co-workers, and others.

    c. Supervisor responsibility for reviewing work products to ensure that productivity, quality, and service are maintained at appropriate levels.

    d. Agreement about how phone calls to the employee's University office and the need for others to contact the employee on remote work days will be addressed.

    e. Specific work-related expenses incurred by the employee, if any, that will be reimbursed by the University. The University does not pay utility costs associated with remote work, including phone or Internet service.

f. For hourly employees, advance supervisor approval if remote work will result in the employee working more than 40 hours in a week (Sunday to Saturday).

g. Employee notification of supervisor and time entry in MaineStreet when disability leave or annual leave will be used during time scheduled for remote work.

2. All University and departmental policies, procedures, and standards of conduct that apply to employees working on campus apply when an employee work remotes.

3. The employee is responsible for ensuring the confidentiality of University data, records, and other information used, stored, or accessed at home. The employee will complete the attached agreement to protect covered data such as personally identifiable information. The agreement outlines appropriate measures to protect data and report security breaches.

4. Unless the employee has use of a UMS issued laptop, the employee is normally expected to provide his/her own equipment for work performed at home. The University is not responsible for damage, repairs, or maintenance to equipment owned by the employee.

5. Any University equipment provided for an employee's home use should be documented as University property and will be returned by the employee when the remote work arrangement concludes or the employee leaves University employment. The employee will bring University provided equipment to a University-designated location for maintenance and repairs.

6. The University will provide supplies for the employee's use while working from home consistent with supplies provided to other employees.

7. As required by University policy, the employee will notify the supervisor and enter time in MaineStreet when s/he uses disability leave or annual leave during times scheduled for remote work.

8. Remote work is not a substitute for dependent care, and family responsibilities must not interfere with work time. During this period of pandemic, we understand that home situations may become more complicated, however, a remote work employee is expected to devote all of his or her attention to University business during their normal working hours.

9. The employee is responsible for maintaining an appropriate, safe work area at home for his or her use. The attached checklist or comparable information should be provided to the employee.

10. The employee will continue to have statutory Workers' Compensation insurance coverage when working remote for an injury that arises out of and in the course of University approved work. An employee who has a work-related injury must report it immediately to the supervisor and other designated officials responsible for Workers' Compensation claims. The University has the right to inspect the site of the injury if a work-related injury is reported.

11. The University is not responsible for damage to employee or third party property or injuries to third parties, unless caused by the negligent acts or omissions of the University.

Self-Certification Checklist
For Remote Work

The following checklist is designed to help you assess the safety of your home office and promote communication and clarify expectations between employees and supervisors regarding safety issues. Please read and answer each question, sign, and review with your supervisor.

Item	Yes	No
Is the work area quiet and free of distraction?		
Are temperature, noise, ventilation, and lighting levels adequate for maintaining your normal level of job performance?		
Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, overloaded circuits, exposed or loose wires)?		
Will the home's electrical system permit the grounding of electrical equipment (a grounded 3-prong receptacle)?		
Are aisles, doorways, and corners free of obstructions to permit visibility and movement?		
Are file cabinets and storage closets arranged so drawers and doors do not enter walkways?		
Are phone lines, electrical cords, and surge protectors secured to prevent tripping or entanglement?		
Is the area in which the University equipment and files will be kept secured from unauthorized users?		
Is your chair adjustable?		
Is your back supported by a backrest?		
Are your thighs parallel to the floor and your knees at a right angle when sitting at your workstation?		
Are your feet flat on the floor or supported by a footrest?		
Is the monitor approximately an arm's length from you? Note: If you work with a monitor that is 17 inches or larger, you may need to move it a few inches farther away.		
Is the top of the monitor slightly below your eye level? Note: If you wear glasses, you may need to position the monitor differently.		
Is the monitor directly in front of you?		
Is the screen positioned to minimize glare and reflections from overhead lights, windows, and other light sources?		

Item	Yes	No
Are documents placed next to the monitor and at the same distance and height as the screen? If not, use a document holder.		
Are the height and angle of the keyboard adjusted to keep your wrist in a straight (neutral) position?		
Are your elbows bent at a right angle when your hands are resting on the keyboard?		
Are the screen's brightness and contrast controls set for optimal viewing?		
Are your head upright and shoulders relaxed when you are looking at the screen?		
Is the mouse positioned close to the keyboard and at the same level?		
Do you have adequate leg room under your desk?		
Are your arms and elbows close to your body when typing?		
Do you use a headset or speaker phone if you use the phone frequently?		
Do you periodically change positions, stand up, and/or stretch?		

Comments/Description of equipment to be used:

Employee's signature: _____ Date: _____

Please give a copy to your supervisor to be placed in your personnel file.

University of Maine System

ADMINISTRATIVE PRACTICE LETTER

SUBJECT: Employee Protection of Data

APPENDIX A: Protection of Compliant Data when using non-University Devices or Networks

Employees who work at home or at non-University locations and employees who use non-University devices will follow the measures below. Employees who telecommute will also follow these measures as part of their telecommuting agreement.

Compliant data includes personally identifiable information, confidential research information, and information that requires protection under law or agreement. Examples of compliant data include: financial records, health records, student educational records, and any information which could permit a person to attempt to harm or assume the identity of an individual such as an individual's name in combination with a Social Security, credit card or bank account number.

1. University-owned Device

An employee who stores, accesses, or emails Compliant Data, other than limited student data as it pertains to particular course (such as faculty records of student activity in a course) will work with Campus IT to ensure the necessary precautions are taken and have encryption enabled on the device. Accessing Compliant Data through MaineStreet does not require working with Campus IT.

2. Non-University-owned Devices

An employee who uses a non-University owned device for work, even if only for University email, agrees to:

- Never store Compliant Data other than student course information on a non-University-owned device. For example faculty may store student data to include class lists and information about current students.
- University data, including email attachments, should never be stored, downloaded or cached on public computers such as those in public libraries or computer cafes.
- Install virus protection software on a computer which is used to access University systems and will manage the system in such a way that the system is monitored and virus signatures are kept current.
- Have disabled web browser's option to store passwords to University systems.
- In the case of a suspected breach, report it to campus IT and, if required, provide access to his or her personally-owned device to UMS staff.

3. Portable Storage Devices

An employee who uses a portable storage device (e.g., portable HDD, memory stick, thumb drive, etc.) agrees that if he or she moves or stores Compliant Data, other than student course information, with a portable storage device, the employee will work with Campus IT to encrypt the Compliant Data storage area and securely erase the device or files when finished using the device for Compliant Data storage.

4. Non-University Network

An employee who has a wireless network at home and might access Compliant Data must secure the wireless network with encryption even if the computer being used is hardwired. An employee who uses non-University networks to access Compliant or Business Sensitive data, will use be sure the connection is secure (for example through https).