

# 9 Telecommuting Tips for Employers as COVID-19 Spreads Across the United States

Article By:

Ashley Prickett Cuttino

---

As COVID-19 continues to spread across the United States, it is anticipated that a large portion of the workforce will be asked to work from home for their own protection and for the protection of others. Working from home (or telecommuting) is not a new concept. However, it will be new for some employees and may strain the resources of a company during the COVID-19 outbreak. Below are some practical tips employers might consider if they ask employees to work from home during the COVID-19 outbreak.

## 1. Implement Voluntary or Mandatory Telecommute Arrangements

The U.S. Department of Labor (DOL) [confirms](#) that you may either encourage or require employees to telecommute as an infection-control or prevention strategy. This includes situations in which employers impose such arrangements based on current information from the Centers for Disease Control and Prevention (CDC) or state or local public health authorities. The DOL notes that telecommuting alternatives may also be used as a reasonable accommodation. (The Equal Employment Opportunity Commission (EEOC) has also discussed using telecommuting as an accommodation under the Americans with Disabilities Act (ADA) during an outbreak in its [pandemic guidance](#).) However, employers may not make such decisions based on protected characteristics, such as national origin, race, gender, age, or pregnancy status.

## 2. Have a Pandemic-Specific Telecommuting Policy

Employers frequently allow employees to work remotely or from home to perform their job duties. However, allowing employees to work remotely or from home is not always possible or beneficial for the employer. As a result, having a telecommuting policy specific to a pandemic, in the present case, COVID-19, is prudent. It is important to make clear to employees that working from home during a pandemic does not mean they are allowed to work from home or alter their regular work schedules after the outbreak is over.

- The policy should make clear which positions are eligible to work from home during the pandemic.
- The policy should make clear how an employee should request to work from home and how

---

the company will inform employees that they are required to work from home. All requests and instructions should be in writing.

- The policy should contain a protocol for when employees may return to work and what protocol will be followed to alert an employer that an employee plans to return to work and/or will be requested to return to work.
- Working outside of the office setting may diminish the employer's control and the employee's accountability. Because some employees will take advantage of the arrangement, the policy should include a clear statement that employees who telecommute continue to be responsible for complying with all employer policies and procedures.
- Ensure your employees understand and know to notify you if they become symptomatic and are no longer able to work and/or need additional accommodations due to illness or to care for a family member. The Family and Medical Leave Act (FMLA) and Americans with Disabilities Act (ADA) will still apply to your employees in a work-from-home situation. If the ability of an employee to work from home changes, application of the FMLA, ADA, and, in some jurisdictions, paid leave laws may become valid.

### **3. Ensure Your Workforce Has the Tools Required to Work from Home**

If your employees need equipment to work remotely, consider a short-term rental of additional laptop computers, scanners, printers, cellular phones and/or multiple monitors installed with the appropriate corporate security for those employees who normally work from company offices.

Employers that choose to allow employees to use their own devices, should consider the cyber-security risks discussed below.

### **4. Consider Cyber-Security**

Working from home can create special challenges to the security of your corporate information. When working in an office setting, employees are normally protected by layers of cyber-security measures. Once an employee begins to work remotely, however, the layers of security may diminish unless specific actions and policies are in place. It is critical to the cyber-security of your operation that a company work with their information technology (IT) department to ensure the same level of security exists for employees working remotely as for those working within the walls of the office.

The Department of Homeland Security (DHS) has provided several tips for working outside of the office:

- Wireless safety is important, and anyone online is vulnerable to attacks. Best practices involve avoiding public Wi-Fi when possible and using a hotspot or encrypted web connection. Using a hotspot will prevent other persons on the same Wi-Fi connection from gaining access to the user's information. Most cellular service providers allow users to set up a mobile hotspot through the user's data plan.
- Ensure all computers/devices with access to your data have an up to date firewall.
- Use a virtual private network (VPN) if possible. A VPN provides a direct connection to the

---

company's normal computer applications such as email, intranet pages, servers, etc. as if the employee was directly connected to the corporate network. A corporate IT department should vet applicable VPN networks and assist with setup if the company does not already have this option. The IT department should also verify that the company's current VPN can handle the excess bandwidth that may be encountered due to the new influx of employees who may need to access the VPN at the same time due to a pandemic.

- Consider additional remote security protections. Depending on the age of your remote desktop application, you may not have the most up-to-date encryption software services available. In addition, employers can take easy steps such as employing strong passwords throughout their remote desktop network and consider additional, different password requirements for certain applications with particularly sensitive information. A remote desktop application should also utilize secure authentication. The most secure networks require a company to employ remote network-level multifactor authentication before a connection is established. Finally consider if all employees need full remote desktop access or whether an employee's access can be confined to certain portions of the network. Any reduction in remote access will reduce the risk of unauthorized intrusion.

## **5. Consider Physical Security**

Employers may want to consider devising a policy regarding the physical security of their property. Such a policy would remind employees to protect corporate data with which they have been trusted. There are many steps employees can take to secure their employers' property. For example, employers can warn employees to never leave a laptop or company-owned or -leased device in their cars or trunks. Similarly, employees should be careful not to lose or misplace thumb drives with company information stored on them or to use a thumb drive if they do not know its origin. It is surprisingly easy to install malware on a thumb drive that is then inserted into a computer and automatically installed without a user's knowledge.

When charging portable devices in public and plugging directly into a USB port, employees can use a USB data blocker to connect to power without exposing the data pins inside the device. These blockers connect power leads but not the data ones thereby preventing data on devices from being stolen. In addition to using blockers, employees can use power cords, which do not allow the transmission of data, or a charging converter, which allows the transmission of power not data, plugged into an outlet.

## **6. Consider Reimbursement for Home-Based Tools and Equipment Used for Temporary Work from Home Arrangements Due to a Pandemic**

If an employer requires remote work from an employee who is not set up to do so, the employer may need to reimburse the employee for any additional phone, internet, or other expenses incurred (beyond what the employee would otherwise have paid for his or her personal use) to enable the employee to telecommute at the company's request. While not directly addressing whether employers must reimburse home expenses used in the course of telecommuting, the DOL advised that if employers require a non-exempt employee to work from home, they may not require the non-exempt employee to pay for business expenses, where doing so reduces the non-exempt employee's earnings below the required minimum wage or overtime compensation. For exempt employees not subject to required minimum wage or overtime requirements, additional phone,

---

internet, or other expenses may be viewed as impermissible deductions under the Fair Labor Standards Act's (FLSA) "salary" basis test. In addition, employers may not require employees to cover such expenses when the telecommuting arrangement is being offered as an ADA accommodation.

In addition, employers should determine any additional requirements imposed by applicable state law. [Illinois](#), [California](#), [Massachusetts](#), [Montana](#) and [New Hampshire](#) have specific state law requirements applicable to employee expense reimbursements.

As a result, it may be helpful for a telecommuting pandemic policy to provide clear instruction on the type of technology-related expenses that will be considered reimbursable. Employers may want to list the percentage of the relevant costs (if not the entire bill) that it will consider reasonable to reimburse. Such a policy may also include the circumstances under which a reimbursement will be allowed and how a reimbursement request should be submitted.

## **7. Employee Pay While Telecommuting**

On March 9, 2020, the DOL's Wage and Hour Division posted a [guidance](#), "COVID-19 or Other Public Health Emergencies and the Fair Labor Standards Act Questions and Answers," addressing wage and hour issues involved in different COVID-19 scenarios. This guidance answers, under the federal wage and hour laws, a number of general questions related to emergencies.

In order to manage the overtime hours non-exempt employees work, a pandemic telecommuting policy (or individual written communication to employees or employee groups) should include several items:

- An expectation that non-exempt employees will continue to adhere to the employer's established overtime policy;
- The expected hours of work for each employee;
- The expected rest and lunch breaks that each employee is expected to take;
- The procedure that non-exempt employees will use to record and report working time;
- The procedure employees will use to communicate with their supervisors, specifications as to when a supervisor should communicate with non-exempt employees, and whether non-exempt employees are permitted to respond to communications outside of the regular work hours agreed upon.

## **8. Workers' Compensation May be Applicable to an Injury at Home While on Work Time**

[Employers are responsible for a safe working environment](#) for their employees regardless of whether their employees work from home or the office. To limit safety issues, employers should make an effort to delineate telecommuting employees' work time and work environment by, for example, requiring employees to designate a specific area at home to serve as an office and to take lunch and rest breaks at designated times. Employers might also want to perform a virtual site check of the

employee's home office to ensure both that there are no potential hazards (such as overloaded extension cords or tripping hazards to name a few) and to ensure that the employee's desk and seating arrangement is appropriately designed.

## **9. Train Your Supervisors on How to Manage Work from Home Employees**

Finally, remote work is different from the typical work structure. Employees who regularly work remotely struggle with unplugging after work, loneliness, difficulties with collaborating and communication, distractions at home, and staying motivated. Managers who do not normally supervise a remote workforce may need guidance on how to best address these issues. The most effective remote workforces retain two key elements found in the normal work environment: connection and collaboration. It is especially important to maintain a personal connection between employees and managers.

Luckily, we live in an era where technology allows us to continue team collaboration and engagement through the use of software related to project management and by video and phone calls. It is important for management to continue to conduct their regular team meetings and one-on-one check-ins with employees who are working from home during a pandemic.

It is also important for managers to set clear expectations for how and when projects should be completed. Goal-based tasks help keep employees motivated and less distracted. They can also help management determine how efficiently remote employees are working so they can address any issues as they arise. It is also important for supervisors to remember to acknowledge good work by remote employees.

## **Conclusion**

Working remotely during a pandemic can be stressful for both employers, which have a need to continue operations, as well as for employees who may be home with children who are out of school or who have never worked remotely before. These practical tips and answers to common questions can help improve an otherwise unpleasant and potentially nerve-racking situation for all involved.

© 2025, Ogletree, Deakins, Nash, Smoak & Stewart, P.C., All Rights Reserved.

---

National Law Review, Volume X, Number 83

Source URL: <https://natlawreview.com/article/9-telecommuting-tips-employers-covid-19-spreads-across-united-states>