This article presents general guidelines for Georgia nonprofit organizations as of the date written and should not be construed as legal advice. Always consult an attorney to address your particular situation.

Tips and Considerations for Your Employees Working From Home During COVID-19

by Matt Higgins

The Governor may have lifted Georgia's state-wide shelter-in-place restriction, but your nonprofit may have chosen to allow all or some employees to continue work remotely. This article provides tips for managing employees and developing a work-from-home technology policy for community-based nonprofit organizations whose employees are working remotely.

COVID-19 has forced organizations to require employees to work from home for an extended period—for many organizations, for the first time. While numerous articles and how-to guides have been written on best practices for developing work-from-home policies, much of the advice they present is infeasible or unrealistic to implement for small nonprofit organizations. This article provides practical solutions tailored to the resources of a typical community-based nonprofit organization to effectively manage employees working from home and develop a work-from-home technology policy to protect the organization's information.

Managing Employees who are Working Remotely

Managers continue to have the authority to oversee an organization's employees while employees are working from home. The lack of physical presence does present challenges, however. Common concerns expressed by employers include lack of productivity, difficulties with communication, and a general lack of managerial oversight over employees. To address these difficulties and effectively manage employees during the COVID-19 pandemic, be flexible and make efforts to maintain consistent communication within the organization.

1. Be flexible.

Be flexible when managing employees during the COVID-19 pandemic. While your organization and its goals should not suffer, managers should be aware that employees are likely to require flexibility to work around issues such as childcare obligations, technology interruptions, or the lack of a suitable home office. Be open with employees about the challenges and concerns with working remotely. So long as work that needs to be done is completed, be prepared to be flexible regarding employees' hours and response times.

2. Maintain consistent communication.

Lack of consistent communication may lead to poor oversight by managers and a feeling of isolation among employees. To maintain effective and consistent communication across the organization, schedule regular one-on-one check-ins between managers and individual employees.

In addition to using these one-on-one meetings as an opportunity to supervise employees, be sure to ask employees about obstacles hindering them from performing their jobs while working remotely. By doing so, your organization can tailor its work-from-home policy to employees' needs. Finally, try to organize conference calls and social activities that connect employees to their colleagues to avoid feelings of isolation.

3. Document actions taken involving employees.

Managers continue to have authority to discipline employees for misconduct or place employees on performance improvement plans while employees are working remotely. Discuss any shortcomings with employees and be sure to document any issues or concerns discussed with employees.

Developing a Work-From-Home Technology Policy

In addition to considering ways to effectively manage employees who are working remotely, consider adopting a work-from-home technology policy. While working from home, employees may be using personal laptops and smartphones to conduct business on behalf of the organization. This raises concerns about lack of control over the organization's information and data security.

1. Why establish a work-from-home technology policy?

Several technology-related risks are posed by employees using personal devices. They include the following:

- *Lack of control* – it is difficult to monitor and control how your organization's information is used and protected when employees are using personal devices.
- *Data security* – employees that are working from home using personal devices may put your organization's information at greater risk. For example, use of unsecured public wifi networks could put your organization's confidential information at risk of theft.
- *Data Preservation* – with employees outside the office, your organization should have policies in place that are understood by your employees to protect documents and other organizational information, particularly if your organization becomes involved in a lawsuit.

2. What should be included in a work-from-home technology policy?

Work-from-home technology policies should address the main risks associated with employees working from home and using personal devices. These include the following:

- *Use of Text Messaging and Personal Email* – prohibit employees from using text messaging and personal email addresses to conduct business on behalf of the organization. Information sent by text message is hard to control, maintain, and recover if lost.

Additionally, if your organization becomes involved in litigation, personal emails will not be protected from disclosure if business was conducted using the personal email address.

- *Use of Public WiFi Networks* – educate employees about the risks of using public wifi networks. These networks typically are not secure, so instruct employees to avoid sending any confidential information when using public WiFi networks.
- *Passwords* – given the risk of employees losing their devices in public spaces while working remotely, require employees to have passwords to access their laptops or smartphones. In addition, require employees to change passwords periodically to add additional security to the organization's information.
- *Consider Requiring "Two-Factor Authentication"* – "two-factor authentication" programs can be cheaply downloaded and installed on employees' personal devices for an additional layer of security. These programs require an additional password to access your organization's email or other information after the device has been opened.
- *Have a plan if employees leave the organization* – Employees may leave your organization while COVID-19 requires working from home, in which case your organization should have a plan to remove confidential information from the employee's personal device or collect organization-issued property (such as confidential files or devices). Consider adding a clause to your work-from-home technology policy permitting the organization to access employees' personal devices for purposes of removing confidential information if the employee leaves the organization.

Conclusion

To operate safely and effectively during the COVID-19 pandemic, your organization should encourage flexibility, maintain consistent communication while employees are working from home and adopt a basic work-from-home technology policy to protect the organization's information. The tips set forth in this article are simple to implement and address many of the major concerns around employees working from home during the pandemic.

Be sure to contact your PBPA attorney for assistance with implementing these work-from-home policies.