Insights, News & Events

ONE YEAR LATER: HOW THE EVOLVING WORK-FROM-HOME CLIMATE PROMPTS REMINDERS FOR TECHNOLOGY BEST PRACTICES

Publication
May 3, 2021

Perhaps no COVID-19 phenomenon will have a more lasting impact than the virtual office. Many employers recently marked the first anniversary of the decision to ask their employees to work from home in an effort to combat the then-novel spread of the virus. By June 2020, 42% of the U.S. labor force was working from home – and that number may linger in that territory for some time. A recent study suggests that among employed adults who say that most of the responsibilities of their job can be done from home, 54% would want to work from home, all or most of the time, after the coronavirus outbreak ends. While this ever-evolving work-from-home climate has challenged employers to embrace technology like never before, you should take note that the conveniences of technology do not come without legal considerations.

The use of technology to communicate with employees and clients, and to generate what it may be argued are business records, raises interesting issues for businesses – particularly in the face of threatened or pending litigation. Whether businesses are beginning to transition their employees to physically return to the office or are continuing to operate virtually, you can avoid potential legal headaches later by taking the time

Service Focus

Privacy and Cyber

Wage and Hour

now to review your best practices and policies as they relate to technology in the workplace.

Email And Texting Continue to Transform Employment Interactions

With less face-to-face interactions and "Zoom fatigue" in mind, many companies have relied almost entirely on email and text communications to reach employees. These casual text exchanges among coworkers may seem harmless when sent but can take on new context in the face of workplace bullying or harassment claims. What one person may construe as a casual joke or playful comment, another may deem offensive.

These days, sexual harassment (or other illegal discrimination) claims are often founded on inappropriate messages or pictures sent via smart phones. Certain communications should never take place over text, and managers communicating with employees over text must remember two important aspects: texts messages are a terrible medium for sarcasm or bad news, and the screenshot of a disgruntled former employee will live on forever.

You should deal with inappropriate or offensive text messages or online posts just as if the comments were made in the office. Employees and their managers must remember that just because comments or jokes are exchanged via text, these communications must still be professional and appropriate. Your workplace policies should be clear in providing that message. Company policy should also encourage employees who receive offensive or otherwise distasteful messages from coworkers, customers, or vendors to bring the messages to their managers' attention, and that employees who send these messages may be subject to termination, even if it was "just a joke!"

Employees Must "Come Home" From Work Even When They're Already Home

While remote work has become the new or even preferred "normal" for many employers, the collective

shift to working from home has driven dramatic shifts in work hours for employees managing jobs, childcare, and wellness routines. As a practical matter, when "the office" became the dining room table or guest bedroom for many, businesses found that their employees remained connected with their work after the traditional 9-5 workday. While this may seem like a pleasing benefit to the efficiency of employees, work-related communications after hours have the potential to expose companies to wage and hour lawsuits.

Non-exempt employees who respond to their employer's text messages or return some work-related emails in their "off hours" may later claim that they were "forced" to work-off-the clock and sue for unpaid minimum wage, overtime, and penalties. Generally, exempt employees who perform any work during the day cannot be docked for missing the day without jeopardizing their overtime exemption. State laws vary on this issue, so it is best to review local guidelines.

To avoid this, you must encourage employees to "come home" from work and save those late-night or weekend texts and emails for the following workday. It may be a best practice to prohibit non-exempt employees from working off-the-clock, even when just responding quickly to a text or email. Direct managers should also be instructed not to send off-hours emails or text messages to non-exempt employees. For exempt employees, you must also avoid reducing pay for absences when they work a part of the day while sick or on vacation, especially if it's important that the employee stays in touch while "away" from the office.

BYOD Policies Can Lead to Indecent Exposure

Employee use of personal electronic devices to conduct their work is not uncommon, but various policies, ranging from encouraging "bring-your-own-device" to outright banning it, have their advantages and risks. The most prominent risk is the possibility that confidential or sensitive information may be shared, stolen, or lost.

If employees must download or access sensitive proprietary information on a computer as part of their work duties, you should provide these employees with a company-owned laptop and obtain a signed agreement from the employee to return it immediately upon termination of employment. Likewise, if employees are required to have a cell phone for work, you should also provide the employee with a phone.

Where a company-owned device is provided, you should also implement a policy to prohibit personal use of the device, in addition to a policy to prohibit the use of their own personal devices to access sensitive business information. You might also consider downloading an application to your devices that allows you to shut down or access a device when lost or stolen.

Providing devices to each employee may not always be the best financial decision for a business. Under these circumstances, it is important to protect the privacy of company information stored on personal devices. When private information is being sent, received, and stored on a device that the employer does not own, then the possibility of data loss or misappropriation is even more present. Additionally, some states impose specific requirements for employer who use BYOD policies, such as providing a minimum phone bill or technology stiped to all employees who use personal equipment to complete work for their employer.

Some employers take the simple step of requiring employees to activate passcode protection on their devices, a procedure that costs nothing but greatly reduces the chance of losing private information. Looking for assistance with an IT team for information about encryption and firewalls that can be put into place is also a proactive way to prevent harmful breaches of privacy.

Similarly, because of the affordability and growing practice of using electronic documents, it has also become increasingly more common to use cloud servers so that employees may use their personal

devices to access company documents, data, and other resources while working from home. Because of how intangible "the cloud" is, it sometimes can be taken for granted how important it is to protect the office's cloud server. You should, at a minimum, have policies against downloading sensitive or protected information from the cloud onto a shared personal device.

Preserving Practices Prevent Potential Production Perils

With all of the above considerations, you must also consider how to preserve a record of all business conducted electronically.

For example, while an electronic text message may appear to be an easy way for employees to request leave or vacation, or quickly provide notice of tardiness or switched shifts, texts are easily lost and (surprisingly) not so easily retrievable, making it difficult to prove a legal defense down the line. You must weigh the value of the efficiency of communicating by text message against the risks it creates. The simplest policy is to prohibit employees from using text messages for business purposes. However, while preserving employees' text messages and emails may be a logistical challenge, in many cases the evidence preserved can be helpful to the company in keeping a record of communications to other employees, managers, company clients, customers, vendors, and other third parties.

As to BYOD policies, it is critical and prudent to regularly assess what level of control you have over your employees' use of personal devices to perform work-related tasks. An employer that fails to preserve relevant information after a duty-to-preserve has been triggered, and then fails to produce responsive documents or messages in discovery, may be sanctioned for spoliation. If the reality of a company's business practices is that employees will be using their personal devices for work, then it is in the company's best interest to implement policies and procedures that

provide the company the right to access and, if needed, the ability to preserve work-related information on employees' personal devices.

While using cloud storage, you should implement programs and policies that keep a record of who has access to documents in the cloud server, when and how that access should be restricted, and what data or sensitive information is both uploaded to the cloud and downloaded from the cloud. Like any other document retention, you must also plan for an electronic process and purging procedure for their electronic documents and records.

Conclusion

One year after the economy saw an abrupt increase in work-from-home professionals, modern business practices indicate that employers continue to rely primarily on technology in their business operations. Nonetheless, in recognizing these changes to your business climate, you must regularly determine whether adapting your policies and practices to this new normal is feasible and prudent, and how these changes might expose you to legal liability – and if so, how to properly preserve evidence for a legal proceeding.

There are a myriad of local, state, federal, and international laws relating to privacy and data protection that should be considered to avoid costly litigation, government enforcement actions, and negative publicity. For more information about technology in the workplace or how it may affect your business, feel free to contact any member of our Privacy and Cyber Practice Group or your Fisher Phillips attorney.