VENABLE® LLP

Articles

January 2014

Bring-Your-Own-Device Programs: Steps to Minimize Nonprofits' Legal Risks

AUTHORS

Armand J. (A.J.) Zottola

Robert F. Parr

RELATED PRACTICES

Technology Transactions and Outsourcing

Labor and Employment

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2014 2010 2006

2013 2009 2005

2012 2008 2004

2011 2007

Nonprofit organizations are increasingly allowing their employees to use their own mobile devices to access, view, download, and transmit work-related materials. While these bring-your-own-device (BYOD) programs may enhance productivity and decrease information-technology costs, these devices also can create certain legal, financial and other risks. Recent reports indicate that almost half of the employers with BYOD programs have experienced a data breach of some kind resulting from employee error or intentional wrongdoing. Even a single breach can lead to financial liability, regulatory penalties, reputational harm, and the loss or unauthorized disclosure of intellectual property. Below is a non-exhaustive list of steps to consider in connection with establishing a BYOD program or allowing employees to use their personal mobile devices for work-related activities.

BYOD Policy

First and foremost, it is important to have a written BYOD policy. Such a BYOD policy should be tailored and customized to meet the operational realities of the particular workplace. In other words, the BYOD policy should addresses all of the activities and related concerns of a particular nonprofit and not amount to a boilerplate, one-size-fits-all policy statement. When creating a BYOD policy, consider the need to address such items as trade secret protection, email/computer/system/document access or usage policies, security policies, device usage policies, sexual harassment and other equal employment opportunity matters, data breach response plans, and employee training initiatives. In addition, consider implementing the policy by obtaining informed consent to the policy statement from all BYOD program participants.

Expectations of Privacy

The use of a single device for work and personal purposes complicates efforts to monitor devices for security or investigative purposes. For instance, personal information may be accidentally deleted when devices are updated remotely, and devices may need to be searched for relevant information in the event of civil or criminal litigation, investigations or enforcement actions. Address employees' expectations of privacy in dual-use or employer-owned devices by explaining how and for what purposes their devices may be accessed or searched.

Data Security

Nonprofits that have access to, process or otherwise maintain certain types of sensitive personal information (*e.g.*, personally identifiable consumer information and nonpublic medical or financial information) must satisfy certain information security obligations imposed by rapidly evolving state and federal laws. These obligations will therefore require nonprofits to consider adequate safeguards for sensitive information that can be made accessible from mobile devices. Be familiar with what types of information must be protected and what types of information will be accessible on mobile devices, and implement the necessary procedures to satisfy applicable legal requirements.

Intellectual Property Protection

Valuable confidential information, patentable ideas, trade secrets, and/or creative works protectable by copyright law may all be accessible on a lost, stolen or intentionally misused employee device. Be sure to set forth rules relating to the use, access rights for, and retention of such information or materials on dual-use or employer-owned mobile devices.

Agency

BYOD programs may expand an employee's scope of employment by combining the workplace with the private sphere. Under certain circumstances, an employer can even be held liable for the tortious conduct or criminal behavior of its employees or the binding obligations and contracts they establish

with third parties. Clearly define what constitutes work and private use to mitigate exposure to this vicarious liability.

Employee Disability

Recent litigation has raised questions about the applicability of the Americans with Disabilities Act (ADA) to organizations engaged in electronic commerce. While the ADA does not expressly apply to BYOD programs, consider having BYOD programs that sufficiently accommodate employees with disabilities.

Labor and Employment Issues

BYOD programs may lead to disputes about overtime pay and expense reimbursement by blurring the lines between regular work hours and personal time. Moreover, BYOD programs could potentially expose a nonprofit to liability under federal and/or state law for an employee's injuries resulting from responding to work-related emails or text messages under unsafe conditions *(e.g.*, while driving a car or exercising). Consider policies for usage and also inform employees about their rights, obligations and limitations with respect to those policies.

Ongoing Effort

Following the above guidance is only the first step in mitigating risks associated with BYOD programs. Nonprofits should regularly track changes in technology, applicable laws and regulations, and workplace culture regarding dual-use devices, and consistently review, update and modify BYOD policies to address reasonably foreseeable risks and issues. And last, but certainly not least, keep employees up-to-date on BYOD issues and policies through written communication and regular training exercises.

* * * * *

Are you interested in learning more about best practices for establishing a bring-your-own-device policy for your nonprofit organization?

Join Venable partners **Armand J. (A.J.) Zottola**, **Ronald W. Taylor**, and **Jeffrey S. Tenenbaum** for a complimentary luncheon/program and webinar, **Implementing a Bring-Your-Own-Device Policy: What Your Nonprofit Needs to Know**, on Wednesday, February 19, 2014. As you are now aware, BYOD policies require thoughtful and careful consideration to prevent BYOD from becoming a nonprofit's "build your own disaster." This program will provide practical guidance for nonprofits on how to reconcile the pros and cons and best practices in crafting an effective BYOD policy for your organization.

Click here for more information and to register for the event.

* * * * *

*For more information, please contact **Armand J. (A.J.) Zottola** at **ajzottola@Venable.com** or **Robert F. Parr** at **rfparr@Venable.com**.*