Electronic Devices At School: What Could Possibly Go Wrong?

Insights
7.01.15

The reality of life for most employees is that most of them cannot make it through an hour, much less a full school or business day, without checking their smartphones, tablet computers, laptops, and other electronic devices. Some schools have sought to manage the chaos by implementing "bring your own device (BYOD)" policies.

The hidden risks and costs of these BYOD policies are significant; this article examines the risks associated with managing the electronic devices of employees of educational institutions. The potential headaches include hidden costs, wage and hour claims, third-party data breaches, accidental communication of confidential information, and invasion of employee privacy.

Increased And Unforeseen Monetary Costs
One of the hidden risks associated with BYOD policies is the actual monetary cost to employers. The assumption has been that BYOD policies save employers money by avoiding the costs of purchasing electronic equipment for employees, instead allowing them to use their own personal devices for work purposes. Employers might also believe they reduce their costs by having employees use their personal data plans for business use.

Any such savings were placed in jeopardy late last year by the decision in *Cochran v. Schwan's Home Service, Inc.* In *Cochran*, an employee filed a class action against his employer on behalf of other customer service managers who were not reimbursed for the work-related use of their personal cell phones. An appellate court held that, under California law, employers must reimburse employees who used their personal cell phones for work.

The court concluded that "[i]f an employee is required to make work-related calls on a personal cell phone, then he or she is incurring an expense .... It does not matter whether the phone bill is paid for by a third person, or at all." The *Cochran* court held that employers must reimburse employees who used their phones for business a "reasonable percentage" of the cost of the monthly plan. While *Cochran* was limited to cell phones, it may be extended eventually to cover other employee-owned devices.

This case is limited to employers in California, and we don't know yet whether it is an outlier or the beginning of a trend that would shift the costs of BYOD practices back to employers.

In an effort to avoid such problems, some employers have created BYOD policies that try to distinguish between personal and business usage of data plans, reimbursing employees for their business use. But such attempts have their own added costs and inefficiencies: employees have to document and log business usage, and employers must review the records before providing a reimbursement. Other employers try to cap the exposure by setting limits on the maximum amount recoverable by the employee or the category of employee who can qualify for such reimbursement. Whether such approaches are legal requires a state-specific analysis of your BYOD policy.

Wage And Hour Risks: An Under-Appreciated Problem

Another hidden cost of BYOD policies is the risk of wage and hour claims that result from employees' use of their personal devices. It was believed that BYOD policies would result in greater productivity, as employees could presumably send and receive work emails and review documents on their own electronic devices not only during normal business hours, but also on evenings and weekends.

This focus on potential round-the-clock productivity can be the first step towards confusion over compensable time and, significantly, a costly wage and hour violation. Consider two basic hypotheticals: if a nonexempt employee uses a cell phone to send and receive work emails outside of the normal work day, the employee could bring a claim for minimum wage or overtime violations against the employer. Such a problem could occur even with exempt employees; if an exempt employee uses a cell phone to send and receive work emails during paid time off, the employer could end up having to compensate the employee for the entire workweek.

The costs to employers of such complications should not be underestimated. If either the nonexempt or exempt employee were to initiate a collective or class action under these hypotheticals, the employer could face a costly legal defense and exposure for all such similarly-situated employees who also used their personal electronic devices.

This in turn, raises the specter of unpaid regular wages, unpaid overtime, statutorily mandated liquidated damages, and the recovery of attorneys' fees and costs. For these reasons, it is important that you carefully analyze the wage and hour implications of your BYOD practices.

Third-Party Data Breach And Dissemination Of Confidential Information

Because educational institutions regularly handle sensitive student information, they can unwittingly create exposure through their BYOD policies by allowing such information to leave a secure, protected environment. The transfer of sensitive, student-focused information to unauthorized third parties could violate state and federal law. Some schools have implemented policies designed specifically to avoid these breaches of confidentiality, expressly prohibiting staff from using their personal electronic devices for work purposes. Whether this is the right move for your institution depends on many factors, but a published policy or procedure placing teachers and staff on notice of their obligations in this regard should be the minimum action taken.

Under The Family Educational Rights and Privacy Act of 1974 (FERPA), education staff must protect the privacy and confidentiality of paper and electronic records containing student information records. Student records include personally identifiable information relating directly to a student that is retained or stored in any way.

FERPA applies to educational agencies and institutions receiving federal financial assistance under any program administered by the United States Department of Education. This includes virtually all public schools, school districts, and many private and public post-secondary institutions including professional schools.

In some cases, students' health records maintained by a school district or individual school receiving funds under a program administered by the Department of Education may present confidentiality challenges under both FERPA and The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Invasion Of Employee Privacy

BYOD policies can also be risky when it comes to employee privacy issues. By authorizing employees to use their own devices for work and subjecting such devices to monitoring and investigation, you risk violating employee privacy rights related to such devices and the electronically stored information residing on them. Schools face risks when their BYOD policies are not coordinated with workplace policies that only permit employers to search personal electronic devices used by employees for work.

For example, a school could unintentionally violate the Stored Communications Act by reviewing employee emails transferred through personal, password-protected email accounts but stored on cell phones, or by ordering an employee to turn over the password to access a social media account on an employee-owned device.

For these reasons, it is important that schools review their BYOD policy to make sure it is consistent with the host of other workplace policies that might authorize employers to access, monitor, and review electronically-stored information residing on the school's computers and electronic communications systems.

For more information, contact the authors at TGallion@fisherphillips.com or 813.769.7510; or at BCossrow@fisherphillips.com or 610.230.2135.

Related People

Brent A. Cossrow
Partner
610.230.2135
Email

Industry Focus

Education

Higher Education