North Bay Schools
Insurance Authority

MEMBER ALERT

"BRING YOUR OWN DEVICE"

Personal Technology Issues and Concerns

Employees commonly use personal "smart phones" (cellular telephones with enhanced capabilities), tablets (iPads/Kindles), personal laptops/computers, and cameras (collectively, "PDAs") for both business and personal use during the work day, a practice known as "Bring Your Own Device," or "BYOD." PDAs may be used to access, download, and store information deemed confidential under federal and state **student** privacy laws (e.g., FERPA), federal and state **medical** privacy laws (e.g., HIPAA and/or CMIA), and **general employee** privacy laws, whether during the business day or while on off-duty hours. Given the capabilities of PDAs, these devices may accidentally or purposefully be used in a manner violating governing laws or Members' policies and placing the employee and the Member at risk for administrative, civil, and (in certain cases) criminal consequences, particularly when the information is used by the employee for a wrongful purpose or confidential information has otherwise been accessed, or disclosed by, an unauthorized individual.

Members' policies and administrative regulations, as well as employee trainings, have not always kept pace with the special risks and responsibilities arising from PDAs. Consequently, this Member Alert provides important guidance on risks, "best practice" standards, and proper management of PDAs in the workplace and when accessed off-duty. In addition to sharing the content of this Alert with employees, Members are also encouraged to (1) review with them the contents of the previously issued Social Media and Cyberbullying Alert (May 2013 ed.), as part of overall training program intending to protect Members and their employees, and (2) give due consideration to updating applicable Board Policies and Administrative Regulations as provided with that Alert.

I. GENERAL ISSUES REGARDING PDAS

When dealing with PDAs, four primary issues arise: (1) costs to replace lost, damaged, or stolen PDAs; (2) reimbursement of telephone or data charges; (3) proper use and access of PDAs during work and non-work hours; and (4) confidentiality obligations associated with PDAs that may be lost or stolen. Each area is discussed below.

A. Responsibility for Lost/Stolen/Damaged PDAs

Absent a collective bargaining agreement that creates a "no fault" obligation by a Member to reimburse some or all of the cost to replace a lost or stolen PDA, costs to replace the device remain solely with employees unless the Member (through the negligence of another employee or volunteer) is facing a potentially viable liability claim. The fact that the device is used for work-related activities does not change this result. Furthermore, because students should not have access to an employee's PDA, a student's actions are not generally the responsibility of the Member. However, loss or damage willfully caused by a student is recoverable from the student and/or his parents through the provisions of Civil Code Section 1714.1/Education Code Section 48904.

B. Reimbursement for Telephone/Data Access Charges

Unless a PDA is a requirement of a particular position (i.e., the job description requires the employee to have a PDA or there is an "expectation"/requirement that the employee will ensure access to communications during non-work hours through such a device), it is the employee's voluntary choice to use such device. The employee has no legal right to demand reimbursement for telephone or data usage, particularly when covered by "unlimited" or similar types of plans where the employee incurs no additional expense by his/her use of a PDA for business and personal use. If such a device is a "requirement" of a position, however, employers should provide reimbursement in an amount/method that fairly addresses the actual costs incurred by the employee for business usage.

C. Proper Use of PDAs

While an employee is permitted to use PDAs during their free time as they deem reasonable and appropriate (although their use of Member-provided network or data access is subject to standard rules and policies regarding

"appropriate" use), employees must not use PDAs during inappropriate times (i.e., teachers taking personal phone calls, or responding to personal emails, during teaching periods). PDA use outside of normal (paid for) work hours can also trigger wage and hour concerns, when the usage is considered other than "trivial." Nonexempt employees, who use PDAs or other devices to check/respond to email, make telephone calls, or engage in other work with the employer's express or implied knowledge or consent, may be entitled to additional compensation.

Members should also ensure that all employees (including volunteer coaches) do not use "texting" capabilities on their PDAs as an alternate method to engage in contact with students and parents. Such communications cannot be tracked and readily retrieved as required by FERPA and the Public Records Act. Instead, "group" emails issued through the Member's IT network (which can be used to send messages to students'/parents' PDAs through MMS/SMS messaging systems, with individual numbers hidden so as not to violate privacy obligations) can be used to address last minute issues while still complying with all legal obligations.

Employees must also ensure that the email designation on the PDA does not default to their personal email address, or that personal email addresses are used to communicate with parents or students. For the reasons noted above, care must be given to ensuring that all communications are issued through the Members' IT network, which also allows the Member to quickly seek to identify inappropriate communications.

D. Confidentiality Obligations and Protective Measures

PDAs access, send, receive and store confidential information (which may include student records/grades; student or employee medical or medication information; student or employee discipline issues, etc.), and take photographs and videos (FERPA concerns) that can present significant liability, regulatory, or public scrutiny concerns. Because these issues are often "work related," both the Member and the employee could face adverse consequences if the information is (a) not properly protected against loss or improper access, and (b) prompt and appropriate remedial measures are not taken in the case of actual or suspected wrongful use or access of the PDA.

Proper protections should -- at a **minimum** -- include updated Member policies that require personal PDAs used for workplace business to have password protection ensuring that applications and content on the device cannot be easily accessed in the case of loss or theft. Failure of employees to meet this relatively simple requirement should properly result in discipline because of the importance of compliance with statutory confidentiality obligations applicable to the employee and the Member. This approach also helps protect employees when students or others seek to improperly access the device. There are cases where a student has stolen an employee's PDA, finding and disclosing thereafter "inappropriate" photographs or texts, or confidential work-related information, resulting in termination of the employee given the content on the device at a school. The wrongful actions of the students are foreseeable, such that the employee should not only ensure that he always maintains custody of the PDA, but that he takes reasonable steps to ensure that access cannot be gained (at least without significant effort).

Another "best practice" approach is to require personal PDAs to download and install mobile device management ("MDM") privacy protection programs, such as those provided by Airwatch, Good Technology and MobilIron. These programs can remotely locate, lock, and/or "wipe clean" a lost or stolen PDA ensuring that confidential information is not improperly accessed (as long as the involved employee promptly notifies the IT Department of the loss or theft). Some of these programs also separate "personal" content from "business" content so that "personal" information is not inadvertently – and, potentially illegally – monitored or accessed by employers. In establishing a defense to a potentially costly data/privacy claim, the use of such software demonstrates reasonable steps implemented to protect against harm or damages.

PDA "back-up programs, such as iCloud and Google Drive, should also be disabled with respect to business related content, particularly if those accounts are (or can be) access or "shared" with others. For instance, if an employee downloads a confidential Excel spreadsheet or letter, or photograph of students, which is then "synced" to a folder that can be accessed or viewed by others, there can be a serious confidentiality breach. Training on these settings, and their proper use, should be a part of each IT Department's routine for new users.

II. CONCLUSION

"BYOD" is now often the standard of choice for both employers and employees, but it is not without substantial risk that should be managed through updated policies, procedures and trainings to ensure the safety of Members, their employees, and those individuals whose confidential information might end up on PDAs.