Solving Your Company's BYOD Office Policy

First introduced more than 10 years ago, smartphones have become ubiquitous in homes and the workplace with many billions of devices in operation.

Entire fortunes have been built on the premise that smartphone users should be able to order a meal or a ride from anywhere at any time. The move to cloud-computing based software as a service (SaaS) programs has allowed people to work remotely, not just by telecommuting from a home office, but from a coffee shop down the street or a beach halfway around the world using their personal smartphones, thus blurring the line between personal and work.

Applications available on smartphones have made our work and personal lives increasingly convenient in many ways, including through GPS directional services and the ability to order almost any product or service at any time, whether at work or at home.

In the rental housing industry, smartphone technology is and increasingly will be used to provide the conveniences that users demand, such as:

- Applicants, residents, site employees, and companies expect to be able to conduct all of their business via their mobile device.
- A prospective resident can take a virtual tour of the property, chat online with a leasing agent, complete, sign, and submit a leasing application, authorize credit and rental history checks, and sign a lease all without ever meeting a leasing agent face-to-face or setting foot on the property.
- A resident can pay rent, submit maintenance requests and interact with property management all through an app on their phone.
- A leasing agent can respond to maintenance requests, provide notification of deliveries, follow-up on inquiries or generally manage the property through the use of the same or a similar app.
- As in-unit residential technology becomes more prevalent, maintenance will be performed through connected smart devices like home security, thermostats, and entertainment systems.

Ian Mattingly, President, LumaCorp., and 2018 NAA Operations Committee Chair, says, "Our associates are in and out of people's homes, leading to privacy concerns and opening us to allegations of improper use. Unsecured and unmonitored devices accessing the thousands of records we control posed a potentially catastrophic risk to LumaCorp. Creating a strong policy around the acceptable uses of, and minimum standards for, personal devices was a critical safeguard."

Mobile applications are improving property and employee

BRING YOUR OWN DEVICE

Security, wage and hour compliance, 'No Facebook' policies and employee privacy among key factors to consider.

BY JENNIFER REDMOND AND BRIAN FONG

performance and efficiency, while making the rental housing industry more connected and accessible.

"Teams work well when they have the tools to work well together," Terry Danner, CEO, SightPlan, and NAA Operations Committee member, says. "Smartphone proliferation has opened a world of opportunities. Serving your customers means doing things well and doing things quickly. Most companies just haven't taken steps to control the text messaging that is occurring, leaving them open to negative consequences."

To meet these needs in the past, companies would issue first BlackBerrys, then iPhones or Android smartphones to their employees. The days of company-issued devices in the rental housing industry are fading for a variety of reasons, from the ubiquity of personal smartphones in employees' everyday lives, to the desire of employees not to carry two separate devices, to the heavy IT costs to maintain a fleet of mobile devices, to the growing social acceptance of blurred lines between personal time and work time. These reasons have led to growing use of personal smartphones for work purposes.

"Personal device policies are a necessity for today's technology-driven environment," Raymond van Beveren, Senior Vice President, Construction and Facilities Services, Pinnacle, and 2017 NAA Operations Committee Chair, says. "Personal devices provide greater efficiency and productivity by allowing employees to communicate, access, track and update information while away from the traditional desktop office."

To craft a BYOD policy, owners and operators must account for the business and personal concerns at the core of allowing employees to use their own personal smartphones to access company systems, including key concerns such as: (1) Network and information security; (2) Employee privacy; (3) Wage and hour compliance; and (4) Policy and procedure compliance. This article explores those competing concerns and offers recommended policy language, recognizing that personal smartphone usage in the workplace is not going away.

Written by Jennifer Redmond and Brian Fong of Sheppard Mullin LLP in collaboration with NAA's Operations Committee. Redmond is a partner and Brian Fong is an associate in the Labor & Employment group at Sheppard Mullin LLP. Redmond and Fong advise multifamily housing firms on how best to comply with the statutory, regulatory and legal challenges that employers face in today's environment.

Article directed by NAA's Operations Committee, whose primary function is to identify emerging operational trends and technologies and operational issues of importance to the apartment industry. The committee serves as a source to gather and share information and develops content and programming to educate NAA affiliates and members on these topics.

NETWORK AND INFORMATION SECURITY

It is extremely convenient and useful to allow employees remote access to company systems for work purposes. At the same time, such access creates serious risks for employers and their clients.

"The use of a personal device introduces many challenges, which a good device policy should address," van Beveren says. "The largest concern from the employee's perspective is that they will lose their privacy by allowing their employer to access their device via remote management software. On the employer's side, the primary concern is related to security. Should devices be stolen or used inappropriately, residents' personal information could be accessed."

From a company perspective, the largest risk of the use of any mobile device, whether company-issued or personal smartphone, is network and information security, including protection of resident and employee information and company intellectual property. In the recent past, there have been many major corporate data breaches across industries.[1] Many more data breaches do not make headlines, and sometimes go unacknowledged for prolonged periods.[2] A data breach costs an organization on average $225 per record lost or stolen, and $7.35 million per organization. These costs include breach detection and resolution, notification to those customers whose data was improperly accessed and the estimated loss of business and customer loyalty. While data breaches can occur through a wide variety of means, the increasing use of cloud-based solutions means that lost, stolen or hacked devices often contain the figurative keys to confidential resident, employee and company information and intellectual property.

Security is a real concern, regardless of whether your network is accessed via a company-issued or personal BYOD device; however, the use of BYOD devices adds an additional layer that must be considered when addressing IT security risks. Company-issued devices are subject to near-complete employer control because they belong to the company. This control comes with the accompanying time and costs for IT departments to monitor, maintain, secure and upgrade each device. BYOD usage, on the other hand, creates the scenario where only certain aspects of the devices are subject to employer control, and only if the BYOD policy adequately accounts for the balance between employer and employee interests in the device.

A great starting point in constructing a BYOD policy is to identify the areas of the device that will be permitted to access company systems, and thus in turn will be accessible by the company for normal business purposes. For example, allowing an employee to access company email on their BYOD device should be conditioned on permitting the company to monitor the use of company email and require that company information not be stored separately on the device. Likewise, allowing an employee to install and utilize a company application, like a property management tool, should be premised on the compa-

IRS Employer Tax Guidelines for Employee Cell Phone Use Issued

On Nov. 22, 2017, the Internal Revenue Service issued guidelines for employment tax issues. Notice 2011-72 points out that cell phones are no longer "listed property," subject to special, heightened substantiation rules.

As non-listed property, cell phones qualify for De Minimis Fringe Benefit rules, which result in no taxation as long as phones or payments for phones are not intended to take the place of compensation and are reasonably related to the employers' business. These technical guidelines include examples of when cell phone payments are or are not taxable compensation.

4.23.5.15.3.2

1. In cases where employers, for substantial non-compensatory business reasons, require employees to maintain and use their personal cell phones for business purposes and reimburse the employees for the business use of their personal cell phones, examiners should analyze reimbursements of employees' cell phone expenses in a manner that is similar to the approach described in Notice 2011-72.

2. Specifically, in cases where employers have substantial business reasons, other than providing compensation to the employees, for requiring the employees' use of personal cell phones in connection with the employer's trade or business and reimbursing them for their use, examiners should not necessarily assert that the employer's reimbursement of expenses incurred by employees after Dec. 31, 2009, results in additional income or wages to the employee. Conditions include that:

- The employee must maintain the type of cell phone coverage that is reasonably related to the needs of the employer's business;
- The reimbursement must be reasonably calculated so as not to exceed expenses the employee actually incurred in maintaining the cell phone; and
- The reimbursement for business use of the employee's personal cell phone must not be a substitute for a portion of the employee's regular wages.

3. Arrangements that replace a portion of an employee's previous wages with a reimbursement for business use of the employee's

ny's ability to review and log the employee's use of the application. It often is necessary to access an employee's BYOD personal smartphone while an employee is employed. This comes up in a variety of situations, including to investigate data breaches, protect intellectual property rights and to preserve evidence for litigation. To preserve the right to such access, the company should be clear that the employee has no expectation of privacy in his or her use of company resources, such as email or other work-related applications available on the personal smartphone.

From there, a mobile device management plan should be implemented to deal with the physical and virtual security risks, and include contingencies such as when, where and how an employee can access company systems, as well as installation of software that will permit the employer the ability to remotely locate and erase the device if it is lost or stolen.

The BYOD policy should also implement basic information security protocols, such as requiring the employee to maintain or authorize the company to maintain any necessary software patches and updates, installation and or authorization of anti-virus and anti-malware programs, requiring that data on the BYOD device is fully encrypted and requiring devices be password protected in line with policies for company-owned technology. The BYOD policy should also specify which operating systems and versions will be allowed to be used as BYOD devices, taking into account which operating systems are not only compatible with other IT resources, but also which operating systems are no longer being updated and/or patched.

Long before the BYOD movement, employers have had to deal with the problem of opportunistic employees taking trade secrets, client lists and other valuable information with them when they transition to new employment. Just as employers take away the keys to a terminated employee's office, a similar response should automatically follow for digital data. Employees should be "locked out" of the system on termination of employment and employers should preserve the right to inspect personal devices that have been used for company purposes to protect company intellectual property. This includes implementing a process to inform IT of the departure, or integrating the mobile devise management software with HR systems to automatically revoke user permissions upon separation, as well as adoption of confidentiality agreements with employees that authorize access to the device for such purposes. While "wiping" the device of a separating employee is an option, it should be taken only if the employee first refuses to turn the device over to IT for inspection.

Network and Information Security Takeaways

- Mobile device management software should be installed on any mobile device that connects to the company network
- Develop a consistently-applied protocol for separating employees to inspect the device and remove any company information

personal cell phone and arrangements that allow for the reimbursement of unusual or excessive expenses should be examined closely.

4. Examples of substantial non-compensatory business reasons for requiring employees to maintain personal cell phones and reimbursing them for their use include:

- The employer's need to contact the employee at all times for work-related emergencies; and
- The employer's requirement that the employee be available to speak with clients at times when the employee is away from the office or at times outside the employee's normal work schedule (i.e., clients are in different time zones).

5. An example of a reimbursement arrangement that does not result in additional income or wages:

An employer has a substantial non-compensatory business reason for requiring the employee to maintain a personal cell phone to facilitate communication with the employer's clients during hours outside the employee's normal tour of duty in the office and reimburses the employee for the use of the phone. The employee uses the cell phone for both business purposes and personal purposes and the employee's basic coverage plan charges a flat-rate per month for a certain number of minutes for domestic calls. The employer reimburses the employee for the monthly basic plan expense to enable the employee to maintain contact with business clients throughout the United States after hours.

6. Examples of reimbursement arrangements that may be in excess of the expenses reasonably related to the needs of the employer's business and should be examined more closely include:

A. Reimbursement for international or satellite cell phone coverage to a service technician whose business clients and other business contacts are all in the local geographic area where the technician works, or

B. A pattern of reimbursements that deviates significantly from a normal course of cell phone use in the employer's business (e.g., an employee received reimbursements for cell phone use of $100/quarter in Q1, Q2, Q3, but receives a reimbursement of $500 in Q4).

WAGE AND HOUR COMPLIANCE

The use of personal smartphones by non-exempt employees creates wage and hour compliance challenges. This is because Fair Labor Standards Act ("FLSA") requires employers to pay all non-exempt employees at least minimum wage for all compensable time worked, and overtime pay at a rate of not less than one and one-half times their regular rate of pay for time worked over 40 hours in a workweek (state law may be even more protective).[3]

Employees who have access to company email and other systems may be tempted or may feel pressure to work when they are off-the-clock. Use of a personal smartphone can exacerbate these issues. For example, an overeager assistant property manager who is seeking promotion might regularly respond after hours to emails from her supervisor. While off-the-clock concerns can be mitigated through the use of features in mobile device management software that "turn off" access to company systems after-hours, BYOD usage may make compliance more difficult. For example, companies cannot require that BYOD personal smartphones be checked in at the end of the workday or during meal or rest breaks. The challenges in limiting access during non-working time or on-call duty can lead to big problems. The magnitude of the issue is illustrated by a recent California Supreme Court decision, in which the Court held that a company policy requiring security guards to remain vigilant, keep their radios and pagers on and respond to incidents during their rest breaks was unlawful, and subjected the company to significant damages and penalties.[4] The settlement in this class-action lawsuit was for $110 million. While the general advice to employers in response to this decision has been to stress to employees the option to turn off or leave company devices at the worksite during breaks, a BYOD device is not susceptible to this approach.

Wage and Hour Compliance Takeaways

- Communicate company policy to pay for all hours worked and recorded
- Inform non-exempt employees they should ignore any company-related messages while on break or after hours
- Reimburse employees for business use of minutes and data usage

Another issue that comes up is reimbursement for work usage of the personal smartphone. In jurisdictions that require companies to reimburse employees for business expenses incurred during employment, companies run the risk that smartphone usage will be considered a reimbursable business expense, even in situations where the employee has an unlimited minutes/messaging/data plan. For example, in a recent appellate decision in California, the court held that companies must reimburse employees "a reasonable percentage of [employees'] cell phone bills," even where employees have unlimited data/minutes plans. However, the ruling did not define "a reasonable percentage."[5]

Given the amount of time employees spend at work, an amount that is 25 percent to 50 percent of typical monthly mobile bill is a good rule for reasonable reimbursement. See "IRS Employer Tax Guidelines" on pg. 46.

Footnotes

[1] Tess Stynes, Essex Property Reports Computer Networks Breach, The Wall Street Journal, September 29, 2014, https://www.wsj.com/articles/essex-property-reports-computer-networks-breach-1411996506; Sarah Ashley O'Brien, Equifax data breach: 143 million people could be affected, CNNMoney (2017), http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html; data breach FAQ, Target Corporate, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ; Panama Papers - How Hackers Breached the Mossack Fonseca Firm, InfoSec Resources (2016), http://resources.infosecinstitute.com/panama-papers-how-hackers-breached-the-mossack-fonseca-firm/.

[2] David McCandless, World's Biggest Data Breaches & Hacks, Information is Beautiful (2018), http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[3] The Fair Labor Standards Act of 1938, as amended, 29 U.S.C. § 201, et seq.

[4] Augustus v. ABM Security Services, Inc., 2 Cal. 5th 257 (2016).

[5] Cochran v. Schwan's Home Service, Inc., 228 Cal. App. 4th 1137 (2014)

[6] Michael Z. Green, Against Employer Dumpster-Diving for Email, 64 S.C.L.Rev. 323, 348 (2012).

POLICY AND PROCEDURE COMPLIANCE

Just as personal smartphones facilitate productive communication, they can also facilitate unproductive or even harmful forms of communication. Email, text messages and social media have become conduits for the distribution of inappropriate and harassing content in the workplace. Some employers have gone to great lengths to prohibit the intersection of social media in the workplace, such as forbidding use of personal social media during working hours. However, there is little evidence so-called "no Facebook" policies are effective, or even complied with. Moreover, there are situations where there may be no clear distinction between an employee checking social media for personal or professional reasons. In fact, it is entirely possible that you checked your Twitter feed during a break in your day and noticed that @NAAhq posted a link to an article on BYOD devices and you decided to download this article to read on your BYOD device during lunch.

Policy and Procedure Compliance Takeaways

- Communicate that company anti-harassment and anti-discrimination policies apply to mobile communications after hours
- Adopt realistic policies for social networking; avoid "No Facebook"-type policies

A better practice is to recognize that BYOD devices grant employees increased access to their personal email accounts and other external content while they are at work, and blurs lines between work and private life. For this reason, employers must be vigilant about updating and enforcing their anti-discrimination and anti-harassment policies, and providing clear and direct harassment prevention training that addresses the impact of BYOD usage. A BYOD policy should explicitly inform employees that the use of BYOD devices does not exempt them from the company's anti-discrimination and anti-harassment policies.

EMPLOYEE PRIVACY AND OTHER LEGAL PROTECTIONS

In many states, employees have a legal right to privacy in their personal smartphone usage. In addition, there are federal and state laws that provide additional protections for employees. For example, the Computer Fraud and Abuse Act (CFAA) is a federal law that prohibits certain unauthorized access of computer data. The right to privacy, CFAA and other laws have been used by employees to sue employers for violations of the right to privacy and other legal protections based on an employer's alleged unauthorized access to personal smartphones used for work purposes.[6] In fact, many employers get into trouble when they treat a BYOD device the same as a company-issued device.

Privacy Takeaways

- Set out clear expectations around areas of the device that are open to company access
- Monitoring may be essential to protect company assets

In the BYOD context, it is essential that employers notify employees that: (1) the company will have complete access to company-related programs and information, such as company email, company data in mobile applications, etc.; and (2) that employees have no expectation of privacy in their personal smartphone to the extent it is used for work purposes. Company access includes remote monitoring, retrieval, data backup, logging, deletion, etc. And, just as areas of company access should be carefully thought through, employers should clarify that those areas of the personal smartphone that are unnecessary for work, such as an employee's personal email, photos and personal applications will not be monitored or accessed without the employee's authorization.

Information provided herein is general in nature and is not legal advice. It is designed to assist rental housing professionals in understanding the issue area, but it is not intended to address specific fact circumstances or business situations. For specific legal advice, consult your attorney.

This is a sample BYOD policy with language incorporating the considerations discussed. It is provided only as an exemplar and is not intended to be used without modification to fit your particular operational situation. Also, the sample policy should be modified to conform with any relevant law particular to your state or local jurisdiction. For a copy of the policy, contact Nicole Upano at nupano@naahq.org.

Bring Your Own Device (BYOD) Policy

The Company has adopted this Bring Your Own Device (BYOD) Policy to meet the needs of our employees. Using your own device for work purposes is not a right, and must be authorized by the Company. In addition, you must read, sign and follow this policy at all times in order to use and continue to use your personal device for work purposes.

Network and Information Security

- Access sensitive business data through Company e-mail and approved applications only. These access points are protected through the security controls discussed below. In all other respects, keep sensitive business data off of your personal device. Sensitive business data includes all documents or data whose loss, misuse, or unauthorized access could adversely affect the privacy or welfare of an individual or Company operations. Delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. Company IT will provide instructions for identifying and removing these unintended file downloads. When in doubt, delete it off of your device;
- Maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer and requested by IT. No "Jail Breaking" the device (installing software that allows the user to bypass standard built-in security features and controls);
- Do not share the device with other individuals or family members. This is strictly prohibited due to the business use of the device (potential access to Company e-mail, etc.). If you are in a situation where you need to share your device with another person, please let the Company know and Company IT will evaluate whether to provide you a Company-issued device;
- Agree to allow the installation of mobile device management software by Company IT. This software allows the Company to remotely locate and wipe the device if it is lost or stolen.
- Report lost or stolen devices to Company within 4 hours or as soon as practical after the device is noticed missing. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- Report any suspected unauthorized access of the device or data breach immediately.
- Your device may be remotely wiped if:
  - It is lost or stolen
  - You separate from your employment without first permitting IT to inspect your device
  - IT detects a data or policy breach, a virus or similar threat to the security of the Company's data and technology infrastructure, as determined by Company in its discretion.
- Smartphones and tablets that are not on our list of supported devices are not allowed to connect to the network. Current devices approved for use:
  - Android Smartphones & Tablets, OS version 7.0 or higher
  - iOS iPhones & iPads, iOS version 10 or higher
  - BlackBerry Smartphones & Playbook, BlackBerry 10 OS or higher
- All devices must be password protected and must lock themselves if idle for more than 2 minutes. You must comply with all Company password policies, including the use of strong passwords, password expiration and password history.

Wage and Hour Compliance

- **Overtime.** Consistent with Company Policy, all overtime work must be approved in advance by a supervisor. Non-exempt employees are paid for all hours worked in accordance with applicable law. Non-exempt employees are responsible for accurately recording their time and are prohibited from working off the clock. Non-exempt employees must have a legitimate business reason for accessing Company network, including Company e-mail, after working time and must receive advance authorization to do so, except in the event of an emergency. Working off the clock, in any form, is strictly prohibited. Any non-exempt employee who works after hours without advance authorization will be paid for such work, but is subject to discipline.
- **Meal Periods and Rest Breaks:** All rest breaks and meal periods are "off-duty." You will be relieved from all work-related duties and free from any Company control during your rest breaks and meal periods. Employees should not conduct any work-related activities during their rest breaks or meal periods, including sending or responding to work-related emails or texts. You are not required to remain "on-call" during your rest breaks or meal periods, unless you are specifically designed as on-call by your supervisor.
- **Dollar Amount of Reimbursement:** Authorized users of personal devices will receive a reimbursement as follows:
  - Voice only - $[XX] per month
  - Data only - $[XX] per month
  - Voice/Data - $[XX] per month
- **Process for Reimbursement:** Complete the Mobile Device Reimbursement Request Form and submit it to your supervisor for approval. Your supervisor will determine if the request meets the criteria and intent of the policy.
- **Reimbursement:** Payment will be made upon presentation of a completed Personal Reimbursement Form along with a copy of the monthly device bill.
- **Use of Device:** You must retain an active device as long as you are receiving device reimbursement. The device may be used for both business and personal purposes, consistent with this policy. Extra services or equipment may be added at your expense. You will not be eligible for device reimbursement during a leave of absence.

Policy and Procedure Compliance

- **Compliance with Company Policies.** You are expected to use your device in an ethical manner at all times and adhere to the Email and Internet Use and other applicable policies as outlined in the Company handbook. This also includes Company policies related to mobile device use while driving and other Company IT policies outlined in the Company handbook.
- **Policy against Harassment:** Displaying sexually explicit images unrelated to work related projects on Company property is a violation of the Company's policy on sexual harassment. You are not allowed to download, archive, edit, or manipulate sexually explicit material while using Company resources, including Company wireless networks, unless relevant to a work related project with approval from your immediate supervisor. If you receive material from outside sources that are sexually explicit and not relevant to work related projects, it is wise to delete or destroy it. If the originator of this material is an employee, you should notify the employee's supervisor or Human Resources. If you believe you have been harassed or if the employee persists in sending the material, you should report the incident immediately in accordance with the Company's Discrimination, Harassment, and Retaliation Prevention Policy.

Employee Privacy

- Company will respect the privacy of your personal device to the extent it is not used for work purposes, and will request access to the device for business purposes only, such as access by technicians to implement security controls, to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads Company email/attachments/documents to their personal device), to protect company intellectual property, or for other business purposes. If you have concerns related to compliance with our security requirements, you may opt to drop out of the BYOD program.
- We will take reasonable precautions to prevent your personal data from being lost in the event we must remote wipe a device. However, we cannot guarantee that such data will be saved, and are not responsible for any expenses or damages that result from the loss of personal data. It is your responsibility to take additional precautions, such as backing up contacts, pictures, messages, etc.

Miscellaneous

- The Company is not responsible maintaining or repairing your mobile device
- The Company is not responsible maintaining, repairing, or reinstalling, any personal software or personal apps on your device

USER ACKNOWLEDGMENT AND AGREEMENT

I acknowledge, understand and will comply with the BYOD Policy. I understand that addition of Company-provided third party software may decrease the available memory or storage on my personal device and that Company is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program. I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by Company IT.

Upon the termination of employment, at any other time that the Company requests, or if I elect to discontinue my participation in the BYOD program, I will: (1) immediately refrain from accessing any Confidential Information stored on my device; (2) allow the Company access to retrieve any Company information or documents stored on my device; and (3) if and when so directed by the Company, permanently delete and erase any Company documents or information stored on my device or provide access to allow the Company to do so; and (4) allow the Company access to the device to remove and disable any Company provided third-party software and services from it.

Employee Name: _____

Employee Signature: _____ Date: _____