KB0054243

Use of Cell Phones/Personal Devices Policy

Providence Shared Services (“ministry”)

Department: Human Resources
Approved by: Chief Human Resources Officer
Date Last Reviewed: 3/25/2025
Date Last Revised: 3/25/2025
Date Adopted: 10/1/2019

Policy Name: Use of Cell Phones/Personal Devices

Scope: All ministry workforce members

Purpose: In keeping with our mission and values, the purpose of this policy is to provide guidance to workforce members concerning the use of cell phones/personal devices.

Terms:

Workforce members includes caregivers/employees, volunteers, independent contractors, vendors, medical staff, interns, students and anyone else with access to the ministry Information Services (IS) domain.

Personal devices are any personally owned devices not issued by the ministry which are used to access company applications and data, including but not limited to: cell phones, electronic tablets/iPads, computers, cameras, watches, ear buds, headphones, and other electronic devices. Shared clinical mobile phones are not considered personal devices.

Policy:

Personal devices may be used for both personal matters and in the performance of work on behalf of the ministry in accordance with the guidelines set forth in this policy.

Personal Use: Personal devices may be used for personal reasons during work time on a limited basis as long as use conforms to safety guidelines, common courtesy, and does not disrupt or interfere with work duties. Personal conversations should be appropriate for the workplace and kept brief. Taking photos and videos of co-workers without their consent, patients, or in patient care areas, while at work is not permitted. Use of personal devices in the workplace must also conform to ministry policies and standards, including security, compliance, HIPAA, patient safety and social media.

Business Use: As a matter of practice, the ministry allows workforce members to voluntarily use their personal devices as part of a Bring Your Own Device (BYOD) Program.

1. **Non-Exempt:** Non-exempt workforce members must not use personal devices for work purposes outside of their regularly scheduled work hours unless specifically authorized by their core leader to do so. Non-exempt workforce members must document in the timekeeping system any time they spend using personal devices for work purposes (including any unauthorized time) to ensure they are paid for all time worked. Failure to comply with these requirements may result in corrective action up to and including termination of employment.
2. **BYOD Program:** As a courtesy to our workforce members, they may voluntarily choose to use their personal devices under the Bring Your Own Device Program. The BYOD Program is intended to provide

workforce members with the ability to use any personal device that the workforce member owns to access ministry systems (computer and network) in a secure environment, where the user logon is authenticated and data is protected. This may allow the workforce member to access email, calendars, contacts, ministry websites, apps or data.

A. **Approval of Devices:** Workforce members who want to enroll in the BYOD Program must request enrollment from their core leaders. Enrollment requests will be approved or denied based on business-related criteria, including but not limited to:
    1. Business need for workforce member to use a personal device for work-related purposes,
    2. Potential or likely interference with job duties,
    3. Compatibility with ministry systems.
B. **Loss/Theft:** Any loss, damage or theft of a personal device is the sole responsibility of workforce members. Personal device users must call the IS Service Desk immediately if their devices have been lost or stolen so that appropriate security measures can be taken. Workforce members also agree to immediately report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of ministry resources, databases, networks, etc.
C. **Security:** No confidential information may be copied/posted to unapproved external applications or websites (such as Dropbox, Evernote, iCloud, ChatGPT, artificial intelligence interfaces, etc.). Personal devices are never to be used to photograph or videotape patients or patient information unless photos or videos are captured with Epic's Photo Capture Program via Haiku or Canto, or other secure mobile applications approved by the ministry, and in all such cases only where such use is consistent with ministry policies.
D. **Personal Cell Phones**
    1. Cell phones that store ministry data must be encrypted, unless the stored data is encrypted by a mobile application. Cell phones are only allowed to connect to the BYOD-designated network or guest network. Devices will be required to maintain the minimum OS version specified by IS. If the version is not maintained, the device will be disconnected from applications associated with the ministry.
    2. **Cell Phone Allowance:** Caregivers authorized to use a cell phone for work-related purposes may be reimbursed proportional to their business use, either through a cell phone allowance via payroll, and/or through the regular reimbursement process. Caregivers should reach out to their core leaders to discuss reimbursement/cell phone allowance and the amount available. Caregivers in certain job categories as designated by the ministry executive leader may be automatically enrolled in the cell phone allowance program. Core leaders should use the Cell Phone Allowance Request tool to submit a request for qualifying caregivers.
    3. If a caregiver's expense exceeds the cell phone allowance or a caregiver does not receive an allowance, reimbursement of the reasonable percentage of the monthly cost of the cell phone plan based on the amount of personal versus business use during the monthly reimbursement period will be available. Proper substantiation is required for reimbursement of expenses exceeding the cell phone allowance, or for those who do not receive the cell phone allowance.
    4. If the workforce member uses a personally owned device on an official business trip internationally, the department will reimburse the total amount of such international calls as provided for in the expense reimbursement policy.
E. **Laptops and Desktops:** Personal laptops or desktops are only allowed to connect to the BYOD-designated network or guest network and must have the following security controls in place:
    1. The device must have all available security patches installed (software and OS) and must be configured to automatically apply critical patches at least weekly.
    2. The device must have an operable anti-malware program with current malware definitions installed, configured to update at least daily.
    3. Personally owned computers are not permitted to store ministry data. They can only be used to access ministry data via virtual environments like Citrix, VDI, or ministry-approved cloud services.
F. **Malicious apps:** Workforce members may be required to remove malicious apps when detected in order to continue accessing ministry data. Malicious applications may be removed at any time without workforce member notice or consent.

G. **Service Desk:** The Service Desk is only available to assist with issues directly related to ministry applications and data. Other issues are the responsibility of the workforce member.
H. **Access:** Administrators may remove the personal device's access to our systems and data at any time. Upon removal of access, the ministry data will be deleted from the device or rendered unreadable. Workforce members who separate from employment are required to permanently delete any ministry data that was not addressed by Information Services.
I. **Privacy:** Workforce members have no expectation of privacy with respect to the applications used to access the ministry systems on a personal device. Workforce members agree to and accept that their access and/or connection to ministry networks may be monitored to record dates, times, duration of access, and other information deemed necessary to maintain compliance and security standards.
J. **Ownership:** Workforce members' contracts with cellular carriers for personal devices are the sole responsibility of the workforce member. However, the data and information created with, transmitted by, and stored on personally owned personal devices by the applications used to access ministry systems is ministry property.
K. **Credit/debit card processing:** Personally owned devices must not be used to accept payment on behalf of the ministry.
L. **Legal discovery:** If used to conduct business matters, personally owned devices may be part of a legal discovery request. Workforce members may need to provide work-related data stored on their personally owned devices to counsel. Subject to legal hold or preservation order, work-related data on a personal device may be required to be imaged or otherwise preserved.
M. **Device sharing:** Personally owned devices with ministry data, and associated passwords, may not be shared with other people including family members.

References:

- Cell Phone Allowance & Bring Your Own Device Program article (core leaders/HR access only)
- Cell Phone Allowance Request (core leaders/HR access only)

Help: For questions about this policy, or assistance with understanding your obligations under this policy, please contact the HR Service Center.

The statements of this policy document are not to be construed as a contract or covenant of employment. They are not promises of specific treatment in specific situations and are subject to change at the sole discretion of the ministry.

This policy is not intended to restrict workforce members from discussion, transmission or disclosure of wages, hours and working conditions in accordance with applicable federal and state laws.

Use of Cell Phones/Personal Devices Acknowledgment

The use of any personal device for work purposes, whether during working or non-working hours and whether on or off ministry premises, must conform to the terms set forth in the Use of Cell Phones/Personal Devices and other ministry policies. I acknowledge the risks associated with the use of my personally owned device for work purposes, and I consent to ministry controls and technical enhancements designed to protect the ministry and its information, networks and data.

Terms and conditions

I agree to the following terms and conditions.

1. I am voluntarily choosing as a matter of convenience to use one or more personal devices for the purpose of conducting ministry work during work time, in addition to personal usage during non-work time.

2. I understand that use of ministry-managed applications on personally owned devices will have security controls enforced on the managed applications containing ministry data.
3. I agree that my contract with any cellular carriers for personal devices and services will be my sole responsibility.
4. If needed for an investigation, I will provide my personal devices to the ministry to access necessary work-related data on the devices.
5. I will use my personal devices in compliance with all applicable ministry policies.
6. I will use my personal devices in compliance with all applicable laws and ordinances, including any laws that limit or prohibit the use of a mobile device while driving.
7. I understand that failure to adhere to these conditions or failure to appropriately safeguard ministry information could result in action against me, including termination of employment, civil action, or criminal prosecution.
8. I agree to hold the ministry harmless for any loss relating to the administration of personal device connectivity to ministry systems including, but not limited to, loss of personal information stored on personally owned devices.
9. I understand the ministry has the right to securely remove all ministry-associated application data on my personal devices at any time. I understand the ministry may at any time and without my prior notice or consent, change or terminate the Bring Your Own Device (BYOD) program.
10. I understand and agree that if I am a workforce member who is eligible to receive overtime pay, that this policy is not actual or implicit approval from the ministry for me to perform work remotely instead of in my designated workplace. If special permission or approval is required for me to perform work other than in my designated workplace and during designated work times, I will obtain prior approval from my core leader. I also agree not to use personal devices for work purposes outside of my regularly scheduled work hours unless specifically authorized by my core leader to do so. I understand that I must document in the timekeeping system any time spent using my personal devices for work purposes (including any unauthorized time) to ensure I am paid for all time worked. I understand that failure to comply with these requirements may result in corrective action up to and including termination of employment.

Acceptance acknowledges that I have read the Use of Cell Phones/Personal Devices policy and that I will comply with its requirements.