POLICY:

This policy establishes the guidelines for issuing a company cell phone to staff, and establishes the guidelines for use of personally owned electronic devices for work purposes:

- It is the policy of CompDrug to consider issuing a company paid mobile phone to employees meeting the criteria and rules set forth in this policy.
- Employees of CompDrug may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cellphones, smartphones, tablets, laptops and computers.
- The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the human resources (HR) department for more details.

Issuance: CompDrug may issue a company mobile phone to an employee whose job function meets one or more of the following guidelines:

Criteria 1:

- Job function requires that the employee be immediately reachable for safety, business continuity, supervision or after hours on-call responsibilities.

Criteria 2:

- Job function is not provided with a work station at a CompDrug service location that includes a desk phone

Criteria 3:

- Employee is assigned to one of the following roles:
    - Any position in the Youth Prevention department in which the employee will be responsible for youth at any location off site
    - Therapeutic Community Program Director
    - Therapeutic Community Alumni Coordinator
    - Strategic Team Member

Change in Job Function: Employees who are issued a mobile phone whose job functions change and no longer meet the guidelines of cell phone issuance will be required to return the mobile phone.

Phone Maintenance: CompDrug takes responsibility for the maintenance of phones issued.

Mobile Device Management (MDM): All corporate issued devices will be enrolled and managed with an MDM tool.

Device protocols

To ensure the security of CompDrug's information, authorized employees are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. Employees must obtain advance approval from their department head and Human Resources to utilize their personal device for work purposes. If approval is granted, employees must sign this policy and present their personal device to IT. CompDrug's IT department must install this software prior to using the personal device for work purposes.

Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network or any work-related data, including email. All BYOD devices that are permitted for work use will need to be screened by IT to verify the operating system. This may require software to be downloaded from the Apple store or Google Play by IT. Once verified, the software can be removed. If the employee does not consent then work email will not be allowed on the device.
Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure Internet sites.

Restrictions on authorized use

Employees whose personal devices have camera, video or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.
While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. CompDrug's policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Employees must adhere to policy 21.059, Use of Phone, Mail Systems, and Electronic Systems, and refrain from using their phones during interactions with patients, visitors, coworkers and during meetings.
CompDrug understands and encourages staff to place a high priority on family and personal interests. While it is prohibited to use cell phones, tablets and personal electronic devices in certain areas and situations, employees may step away from the area to place and receive brief calls or text messages. Employees should provide individuals who may need to reach them in emergency situations with the CompDrug main phone number so that they may be reached when necessary.

This policy applies to personal cell phones, tablets and personal electronic devices and CompDrug-issued cell phones, tablets and personal electronic devices.
Nonexempt employees may not use their personal devices for work purposes outside of their normal work schedule without authorization in advance from your department head. This includes reviewing, sending and responding to e-mails or text messages, responding to phone calls, or making phone calls.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management, without advance approval.
CompDrug reserves the right to deactivate the company's application and access on the employee's personal device during periods of unpaid leave.
An employee may not store information from or related to former employment on the company's application.
Family and friends should not use personal devices that are used for company purposes.

Privacy/company access

No employee using his or her personal device should expect any privacy except that which is governed by law. CompDrug has the right, at any time, to monitor and preserve any communications that use the CompDrug's networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that CompDrug's resources in these areas are being use according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

Mobile Application Management (MAM): Mobile application management will be enforced on all corporate and personal devices that access company data resources.

Security: Employees who are issued agency cell phones or who utilize personal phones for agency business are responsible for the security of the device. All devices must be assigned a pin or passcode. Employees must notify Information Services immediately of any lost, stolen or damaged devices.

Safety: Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times.
Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations involving traffic, inclement weather or unfamiliar areas.
Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.
Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost, stolen, hacked or damaged equipment
Employees are expected to protect devices used for work-related purposes from loss, damage or theft.
In an effort to secure sensitive company data, employees are required to have "remote-wipe" software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.

CompDrug will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged

Appropriate Use and Privacy: See 21.042 Computer and Email Usage and 21.059 Use of Phone, Mail Systems, and Electronic Systems.

Termination of Employment: Upon termination of employment, the issued device will be collected back. Personal phone numbers ported into CompDrug's cell phone plan prior February 12, 2018 will be released upon termination. The exiting employee will be provided with a two week period (14 calendar days) from the date of termination to re-establish personal cell phone service for the phone number (if porting applies) and to obtain a cellular device. At day 15 days post termination, the number will be terminated and the device must be returned to CompDrug.

Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.

Phone Numbers: Effective February 12, 2018, CompDrug will not port personal phone numbers into the agency cell phone plan. If a mobile device is issued, the phone will be assigned an existing agency phone number or a new phone number will be established.

Upgrade/Replacement: The agency will replace agency-owned devices that are no longer in working order or that are out of date.

Use of Mobile Phones While Operating Motor Vehicles: See 15.036 Wireless communication device policy.

Mobile Platforms Supported: Android and IOS

Business Exceptions: The CEO may document in writing exceptions to this policy.

Violations of Policy: Employees who have not received authorization in writing from CompDrug management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow CompDrug's policies and procedures may result in disciplinary action, up to and including termination of employment.

CompDrug reserves the right to amend, change or terminate the mobile phone issuance policy at any time.

Revision History

EFFECTIVE:	11/10/2016
REVISED:	**05/14/2018; 02/14/2019**
Reference:	