*NOTE: This policy is not mandated by New York City/State or Federal law, and reflects the operational preferences of the author only.*

**PERSONAL DEVICE POLICY**

[Organization Name] does not object to employee use of personally owned devices (e.g., smart phone, tablet, lap top, computer or other device) for work purposes, including to connect to [Organization Name]’s electronic communications systems, send and receive email and access additional resources. The use of any personal devices for business purposes must conform to this policy and [Organization Name] reserves the right to restrict or limit such use of personal devices.Each employee is responsible for using his or her personal device in a sensible, productive, ethical, and lawful manner. **This policy applies to work performed on a device on [Organization Name]’s** **behalf during working and nonworking hours, on and off of [Organization Name]** **premises.**

No Expectation of Privacy:
Any emails, files, data, documents, facsimiles, telephone conversations, voice mails, social media posts or messages, or other communications or content created on, transmitted through, received on or printed from, or stored or recorded on a personal device for [Organization Name] business or on behalf of [Organization Name], are the property of [Organization Name], regardless of who owns the device. As it does with all [Organization Name] communications,[Organization Name], in its sole discretion, reserves the right to monitor, access, retrieve, read, disclose, and/or delete, without further notice, any communications or content **created on, transmitted through, received on or printed from, or stored or recorded** on a personal device, to the fullest extent permitted by applicable law**.** Therefore, employees should have no expectation of privacy whatsoever in any communications or content created on, transmitted through, received on or printed from, or stored or recorded on a personal device if the employee uses the device for business purposes.

[Organization Name] may also store copies of such content for a period of time after it is created, and may delete such copies from time to time without notice. In addition, [Organization Name] may obtain and disclose copies of such content or the content of the entire device (including personal content) for litigation or investigations and may share such content with government officials or third parties.

Employees acknowledge that the use of any personal device for [Organization Name] business or on behalf of [Organization Name] is at the employee’s own risk, and [Organization Name] will not be responsible for any losses, damages or liability arising out of the use of any personal device for [Organization Name] business or on behalf of [Organization Name] under this policy, including any loss, corruption or loss of access to or use of any content, the device, its software or its functionality.

Costs and Reimbursements:
Employees who choose to use personally owned devices for work purposes must pay for their own device costs under this policy. [Organization Name] does not provide technological support for personal devices. The employee acknowledges that the employee alone is responsible for any repairs, maintenance, or replacement costs and services associated with use of a personal device.

Appropriate Use:
Employees who choose to use personally owned devices for work purposes are required to do so in accordance with all [Organization Name] policies and employee handbook/s, if any. Employees may not use any personal device in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by Federal, state or local law.

Any employees who discontinue use of their personal devices under this policy or leave [Organization Name] employ, must remove any of the [Organization Name] work product or sensitive business content from the employee’s personal device.

**[Organization Name] prohibits employees from talking, texting, e-mailing or otherwise using a device to conduct [Organization Name] business while operating a vehicle.** Employees must also abide by all applicable legal prohibitions on the same when using personal devices for [Organization Name] business or on behalf of [Organization Name]. 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.

Confidentiality and Proprietary Rights:
[Organization Name] confidential and proprietary information and intellectual property, including trade secrets, are extremely valuable to [Organization Name]. You must treat them accordingly and not jeopardize them through your use of your personal device. Disclosure of the [Organization Name] confidential and proprietary information to anyone must comply with all applicable policies.

Security Considerations:
To protect [Organization Name] and its partners’ confidential or proprietary information from being lost or becoming public, employees must immediately report any device used for [Organization Name] business or on behalf of [Organization Name] that is lost, stolen, accessed by unauthorized persons or otherwise compromised.

[Organization Name]’s Electronic Communications Systems Policy, Confidentiality Policy and Social Media Policy apply to all uses of personal devices for [Organization Name] business or on behalf of [Organization Name]. In addition, employees using personal devices for [Organization Name] business or on behalf of [Organization Name] must comply with the following requirements:

1. At all times, employees must use their best efforts to secure personal devices against loss, theft, or unauthorized use or access.
2. The device’s original operating system must be maintained and kept current with security patches and updates.
3. Employees may not use cloud-based backups that allow [Organization Name]-related data to be transferred to unapproved third parties.
4. No employee shall knowingly disable any network software or system identified as a monitoring tool.
5. Upon termination of employment for any reason, or at any time upon request, an employee may be required to produce the personal device in order for IT to remove, ifapplicable,[Organization Name] configurations from the device. All [Organization Name] data on personal devices must be removed upon termination of employment.

Failure to comply with any provision of this policy may result in disciplinary action up to and including termination of employment.