USE OF TECHNOLOGY AND PRIVACY POLICY

[Organization Name] supports the appropriate and responsible use of cellphones and technology by our employees when deemed necessary. This policy outlines the terms for the appropriate use of personal cell-phones, internet, and other personal devices while at work and while interacting with clients. The purpose of this policy is to ensure that employees utilize cell-phones and other personal devices only when necessary and remain diligent in keeping client information private and confidential to mitigate any potential risks to the organization.

DEFINITION

* **Technology** refers to any form of communication tools and networks, such as but not limited to devices, software, email, and the internet, that are used in performing work-related tasks and functions within and outside the premise of [Organization Name]. This may include but is not limited to: personal computers, cell phones, smart watches and other personal electronic devices.
* **Electronic Communication System** pertains to [Organization Name]’s existing program, database and channel where all employees can access all forms of communication, files, and documents.

POLICY

Employees are expected to use company computers, email, technology, and access the internet for employment purposes only. Employment purposes refers to duties required as outlined in the employment agreement, job description or as directed by the organization. Use of the organization's network for personal activities is not acceptable, unless authorized by management.

Employees are free to use personal cell phones, computers, or other personal electronic devices during designated breaks, lunch and off-work times. Any activity that reflects negatively on the organization, compromises client privacy, poses a danger to company equipment, or conflicts with other company policies, such as the Social Media policy, will not be permitted and will be addressed accordingly with our corrective action process.

Ethical Conduct

Employees must always conduct themselves appropriately when accessing the company’s technology and electronic communication system. No form of the company’s technology may be used in an offensive, harassing, illegal, or defamatory manner at any time.

Restricted Use

The following actions are restricted on the company’s electronic devices and internal network:

* Use of personal electronic devices during work time, unless otherwise authorized to do so.
* Internet sites which are deemed to be inappropriate will not be permitted to be accessed on the Company’s electronic devices and will be subject to disciplinary action.
* Company email must only be used for employment purposes. Emails will only be sent or received to and from people as required for work purposes.
* Company email is subject to the organization’s policies, including: *Workplace Violence, Harassment and Discrimination, Appropriate Workplace Conduct and Confidentiality, etc*.
* If an inappropriate email or link is received, it must be deleted immediately, and the email must be reported if sent internally. If the email is forwarded, the employee forwarding it will be subject to appropriate discipline.
* Employees should refrain from downloading files, music, videos, pictures, etc. not required for employment purposes on company devices or internal databases.
* Conducting unapproved business for any alternate sources of employment, compensated or otherwise, or for any home-based business at any time.

Software and Communication System and Data

Employees are responsible for the use and security of their company computer, including email accounts, and/or any other technology assigned to them. Employees should use appropriate passwords and protections and ensure their computer is secured when unattended.

* Employees shall only use all of the [Organization Name] software for work-related tasks and functions. Any unauthorized use or duplication of this software is strictly prohibited.
* Employees shall not install or run security programs or utilities unless specifically instructed to do so.
* Employees must comply with copyright and licensing restrictions on any information which has been downloaded or is protected by the organization.
* Employees are prohibited from using protected materials (copyright material, branding and/or logos) without prior express written permission.
* Employees may not allow others who are not authorized users to access and utilize company equipment or software.
* The use of any non-company licensed, third-party, or encryption software tools that may access [Organization Name]’s confidential information is prohibited unless authorized to do so.

Use of Personal Devices (e.g., personal cell phones)

* Employees’ personal devices are generally not given access to the company’s electronic communication system unless the device is approved, authorized, or provided by the company for work-related tasks and functions.
* Employees may not use their personal cell phones during work hours for personal purposes, unless otherwise approved my management or unless on a scheduled break
* [Organization Name] retains the right to monitor staff members for cellphone use during working hours.
* Employees are prohibited from storing, accessing, or sharing any private information, including but not limited to: client’s personal information and the organization’s confidential or proprietary information on their personal computer, cell phone, smart device or any other personal electronic device.

Breaches of this Policy

Breaches of this policy may lead to disciplinary action, up to and including termination of employment.