Technology Use Policy

This Technology Use Policy covers the use of our equipment, software, organizational and individual accounts, login credentials and passwords, online resources, and other information technology (collectively, "IT Resources"). If you have questions about this Policy or about what is appropriate or acceptable, you should consult the IT Director or the Chief Information Officer.

The intent of this Policy is to ensure that the use of our IT resources supports our mission and protects our clients, our organization, and everyone who uses our IT resources from illegal or harmful actions by others, whether done knowingly or unknowingly. This requires complying with relevant legal, contractual, professional, and policy obligations whenever we use our IT resources. This also requires that individuals not interfere with the appropriate use of our IT resources by others.

This Policy broadly covers all of our IT resources, including our hardware, software, organizational and individual accounts, and content, and includes but is not limited to our networks, internet connectivity, systems, equipment, computers, devices, telephones, data, files, content residing in any of our IT resources, records of our organization, and the information in those records regardless of the form or the location. Our Mobile Device Use Policy sets forth further information related to mobile devices owned by [redacted] such as laptops, cell phones, and other equipment.

Every employee, VISTA, intern, and volunteer ("employees, interns, and volunteers") who uses our IT resources is responsible for reading and complying with this Policy, and for using reasonable care when using our IT resources. Any violation of this Policy may result in disciplinary action up to and including termination. Employees, interns, or volunteers who misuse or abuse our IT resources may be responsible for reimbursing [redacted] for the costs incurred. In some instances, the misuse or abuse of IT resources or the unauthorized disclosure of information may violate the law.

Independent contractors, consultants, and other third parties who use our IT resources must agree in writing to reasonable and appropriate use of our IT resources, as that use relates to the work they are doing for us, before they receive access to our IT resources. Such persons also should agree to indemnify, defend, and hold harmless [redacted] for any damages flowing from their misuse or abuse of our IT resources.

This Policy also applies to any personal devices that connect to our IT resources or to our organizational or individual accounts.

Employees, interns, and volunteers must immediately report any loss or damage of any IT resources, and any personal device that connects to our IT resources or to our accounts, to our IT work group in person, by calling [redacted], or by emailing [redacted].

Privacy and Confidentiality of Records and Electronic Communications
Employees, interns, and volunteers are responsible for ensuring that their handling of records that contain Personally Identifiable Information ("PII") is consistent with this Policy. Before exchanging data that includes PII with any third party, employees, interns, and volunteers must take appropriate steps to remove metadata, encrypt the information, or share the information via secure methods, as applicable. Records that do not contain PII must be handled with reasonable care and due regard for privacy and confidentiality.

Employees, interns, and volunteers must exercise caution to protect information from unauthorized disclosure or access, particularly with regard to electronic communications because such communications can be distributed easily to a vast audience and because such communications are under the constant threat of unauthorized access.

When [redacted] decides there is a basis for doing so, [redacted] may access electronic or other records (including paper files) or monitor the employee's, intern's, or volunteer's use of IT resources without the consent of the employee, intern, or volunteer. For example, [redacted] keeps and may monitor logs of internet usage, web traffic, and email communication. No employee, intern, or volunteer should have an expectation to privacy in their use of IT resources or the information stored on IT resources.

Security of Information
Employees, interns, and volunteers who use IT resources must take reasonable steps to protect these resources from unauthorized modification, disclosure, access, and destruction. Data and software are to be protected, regardless of the form, medium, or storage location of the information. The level of protection shall be commensurate with the risk of exposure and with the value of the information and the IT resources. Our proprietary business information must not be divulged to outside parties. Any written, electronic or oral transfer of proprietary information must have prior approval of the Chief Executive Officer/Executive Director or their designee.

Preservation of Information
Employees, interns, and volunteers have an obligation to provide accurate, reliable information to authorized recipients and to preserve records created in the course of ordinary business. In addition, upon direction from the Chief General Counsel or Chief Information Officer or their respective designees, records must sometimes be preserved for prescribed periods of time for litigation or other legal purposes.

Approved Use of IT Resources
Employees, interns, and volunteers are obligated to use our IT resources in accordance with all applicable laws, regulations, ethical obligations, and policies, and in ways that are responsible, ethical, and professional. Use of our IT resources is restricted to business purposes and incidental personal use. Incidental personal use may not interfere with business purposes, nor may it result in additional cost to our organization. For example, employees, interns, and volunteers may make

incidental personal use of our internet bandwidth as long as it does not interfere with business purposes or result in additional cost. At no time may any employee, intern, or volunteer make use of our IT resources to conduct activities that are unlawful or prohibited by the Legal Services Corporation.

Our IT work group is responsible for purchasing, maintaining, setting up, and moving all IT resources, including but not limited to computers, monitors, telephones, and organizational and individual accounts. Exceptions for employees, interns, and volunteers to move their own equipment may be made by IT as needed. Employees, interns, and volunteers who desire additional equipment or software, replacement equipment or software, new organizational or individual accounts, or updates to existing organizational or individual accounts, must contact the IT work group.

Our IT resources must be used in a manner consistent with our status as a non-profit organization, and cannot be used for the benefit of personal businesses or other organizations unless authorized by the Chief Executive Officer/Executive Director or their designee.

Personal Devices Used For Business Purposes

Employees, interns, and volunteers who use their personal devices to support our mission must comply with this Policy. Personal devices that connect to IT resources must be protected by the minimum requirements established by the IT work group such as a firewall, current security updates, patches, and antimalware definitions. Employees, interns, and volunteers are responsible for backing up personal data on their personal devices. Any personal device that connects to our IT resources is subject to being remotely wiped if lost, stolen, or other circumstances warrant such action. As noted above, employees, interns, and volunteers must immediately report any loss or damage of any personal device that connects to our IT resources to our IT work group in person, by calling [redacted], or by emailing [redacted].

Interference with IT Resources Prohibited

Employees, interns, and volunteers must not interfere with, disrupt, or alter the integrity of our IT resources. Employees, interns, and volunteers must obtain approval from the IT work group before installing any equipment or software connected to our IT resources. Restricting or denying access by legitimate users of our IT resources, and destroying, altering, or disclosing without authorization any data, programs, or other content that belongs to others but that is accessed through our IT resources, is prohibited. Unauthorized access or interception of electronic communications is prohibited by this Policy and may also violate the law. [redacted] may block an individual or group's access to its IT resources in order to protect [redacted], its clients, its IT resources, and the information contained therein.

Restrictions on Use of Certain IT Resources from Outside Sources

Special restrictions are placed on the use of IT resources as required by law, trade secret, or by contract in the form of a license or other agreement. If you are unsure whether a proposed use is appropriate, consult the IT Director or the Chief Information Officer.