[ORGANIZATION NAME] Technology Policy

The [ORGANIZATION NAME] is a large legal aid program with numerous technology solutions in place to meet the varied needs of our staff and clients. It is imperative that all employees be familiar with our Technology Policies and abide by them. Managers, please ensure that you go over these with new staff and students at onboarding. If anyone has questions, please contact [[ORGANIZATION NAME EMAIL]](mailto:MAP-IT@lsscm.org). Thank you for doing your part to ensure that our equipment is taken care of and our policies are followed - it will significantly increase the security of our systems and sensitive client data, reduce the amount of technology problems people encounter, and keep our services operational.

# OWNERSHIP OF PROGRAM EQUIPMENT AND TECHNOLOGY

## **Ownership.** All [ORGANIZATION NAME] equipment and technology is owned by [ORGANIZATION NAME] and subject to monitoring by IT staff and management. All technology systems, including computers, computer software, telephone systems, fax machines, copier machines, voicemail systems, email systems, and Internet access systems within the [ORGANIZATION NAME] offices are the sole property of [ORGANIZATION NAME]. No individual staff member has any proprietary or confidential interest in any materials stored or copied in any office files or systems, including voicemail and email. Any material in any [ORGANIZATION NAME] system may be monitored, copied, or quarantined by the program management at any time. Additionally, staff should not store non-work-related files on their computer hard drives or on a [ORGANIZATION NAME] network.

## **[ORGANIZATION NAME] Access to [ORGANIZATION NAME] Devices.** In order to assure that the primary use of these systems is the provision of legal services to low-income clients in compliance with program policies, program priorities, and program grant requirements, [ORGANIZATION NAME] has the right to monitor and control the use of all its property, equipment, and systems. [ORGANIZATION NAME] may access all aspects of all systems, without the consent of the user, at any time. When accessing equipment is required, [ORGANIZATION NAME] will attempt to notify staff beforehand who are actively employed and in good standing unless doing so causes a security risk or immediate action is required to maintain the integrity of [ORGANIZATION NAME] systems and data. The specific circumstances when [ORGANIZATION NAME] may access equipment include but are not limited to:

1. When necessary to identify or diagnose system or security vulnerabilities and problems or otherwise preserve the integrity of any system; or
2. When such access to systems is required to carry out essential business functions of [ORGANIZATION NAME]; or
3. When there are reasonable grounds to believe that a violation of law or a significant breach of [ORGANIZATION NAME] policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
4. When the user’s employment at [ORGANIZATION NAME] has ended and there is a business reason to access the system.

## **Installing Software on [ORGANIZATION NAME] Devices**. [ORGANIZATION NAME] staff may install any applications or software on their assigned device which is available on the Company Portal. Before installing any other applications or software (not available on the Company Portal) on their assigned device, staff must request permission from both their managing attorney and [ORGANIZATION NAME]-IT. Any new applications or software must be installed by [ORGANIZATION NAME]-IT unless they have specifically designated this task to an office Computer Responsible Person (CRP). Adding an application or software to a shared device can only be done by [ORGANIZATION NAME]-IT after being requested by a Managing Attorney.

1. **Care of Program Equipment**. Staff are expected to exercise great care for [ORGANIZATION NAME] equipment. This includes: not eating or drinking near your keyboard or laptop; carrying laptops in protective cases; keeping laptops secure at all times and storing at proper temperatures; all cords should be used and stored so they won’t be damaged or create trip hazards; etc. When [ORGANIZATION NAME] loans shared equipment to an employee (i.e., projectors or shared laptops), the equipment is to be returned in its original condition. This includes all peripherals and accessories (mice, cables, remotes, etc). The program may charge staff the cost of repair for the loss of or damage to program property if the damage is caused by actions of staff that are intentional, negligent, or in violation of this policy. In the event [ORGANIZATION NAME] equipment should be stolen, misplaced, or compromised in any way, employees are required to contact Amanda Revels and Scott Ellis IMMEDIATELY at [[ORGANIZATION NAME]-it@lsscm.org](mailto:map-it@lsscm.org) and to their direct email addresses if it is outside of regular work hours[.](mailto:map-it@lsscm.org)
2. **USB Keys**. Some employees and students are given a USB security key to enable access to shared laptop or desktop computers. Replacement of a lost security key will result in a $20 fee to the employee to cover the cost of a new key. Local Managing Attorneys (who may delegate this task to the CRP) will assign USB security keys to students and track the return of them at the end of the term. Any employee or student who loses their security key or does not return it is responsible for the $20 fee.
3. **Personal Use of [ORGANIZATION NAME] Equipment and Technology**. Employees are permitted reasonable personal use of program equipment provided that:

* this use occurs on the employee’s personal time;
* the employee reimburses the program for any direct costs associated with the use;
* this use doesn't interfere or conflict with any other provision of this policy or with [ORGANIZATION NAME]'s programmatic use of the property, equipment, or systems.

Excessive use of technology resources for non-work-related purposes, such as game playing or downloading media files is prohibited. [ORGANIZATION NAME] email accounts are to be used for [ORGANIZATION NAME] program purposes only; staff are expected to have a non-work email account for their personal email correspondence.

1. **Prohibited uses of [ORGANIZATION NAME] Equipment and Technology**. For-profit use of [ORGANIZATION NAME] equipment and technology is strictly prohibited. [ORGANIZATION NAME] employees are not permitted to use [ORGANIZATION NAME] equipment for LSC-prohibited purposes at any time. [ORGANIZATION NAME] employees are not permitted to let anyone who is not a [ORGANIZATION NAME] employee use [ORGANIZATION NAME] equipment.
2. **Assignment and Use of Shared Laptops**. All offices have one or more office laptops intended to be shared by staff (“shared devices”). The laptops can be checked out by any employee needing a laptop for a specific event or while their primary device is out of service. Shared laptops are not to be used for general daily use, or taken home (except between days of continuous use) - they must be available for general office use. Each office manager (who may delegate the task to the CRP) must track the location and working order of shared laptops at all times on the Justice Server devices page.

# INTERNET USE

1. **[ORGANIZATION NAME] Internet - Work Related Use Only**. The program's connection to the Internet exists to assist us in our legal work, including contact with funders, research, email, etc. Except as provided in Section I (F) of this policy, all Internet use shall be work related.
2. **Prohibited Uses of [ORGANIZATION NAME] Internet**. All internet use is traceable. No staff person should use program equipment for purposes prohibited by program policies or that could not be reasonably explained to persons outside the program. Employees are prohibited from using any piece of [ORGANIZATION NAME] equipment to view material that is pornographic in nature or for any use of the internet that violates civil or criminal law.

Unauthorized use of peer to peer file sharing services (e.g., BitTorrent, Shareaza, eMule, uTorrent, etc.) while connected to any [ORGANIZATION NAME] network, or on any personal device that has [ORGANIZATION NAME] Sharepoint synced to it, is prohibited.

1. **Remote Work at Home**. If employees use wifi on their home network, they must use a strong password (numbers, letters, symbols) of at least 6 characters and WPA2 encryption. The encryption key should not be shared with anyone outside the employee’s household including occasional visitors or friends. If your router only has WEP wifi security you should consider upgrading to a new router (WEP passwords can easily be hacked by a neighbor or someone parked near the home).
2. **Remote Work away from Home**. If an employee plans to work from a remote location other than their home, they must download OpenVPN from the Company Portal. When using public wi-fi connections at coffee shops, airports, hotels, ect., employees should only connect to the internet using OpenVPN. Please set it up and test it at least 24 hours before you travel and anticipate needing it for the first time to ensure it is working properly.

# USE OF PERSONAL DEVICES FOR [ORGANIZATION NAME] WORK

[ORGANIZATION NAME] is a hybrid work environment, meaning that many employees work remotely some of the time. Once an employee has been assigned a [ORGANIZATION NAME] laptop, they should use the assigned device for all work, both remote and in-office. In addition to the Equipment provisions of the [ORGANIZATION NAME] Remote Work Policy (Section C), the following rules apply to use of personal devices for [ORGANIZATION NAME] work:

1. All [ORGANIZATION NAME] employees are assigned a desktop or laptop computer (assigned device) that is adequate to perform their job duties. For this reason, generally and absent any temporary policy noting otherwise, personal devices are not permitted to be used at [ORGANIZATION NAME] offices unless there is a specific business case for doing so (such as a work need to use a program that is not available on a [ORGANIZATION NAME] device). Employees must receive permission from [ORGANIZATION NAME] IT before using a personal device for work. This applies to [ORGANIZATION NAME] employees, volunteers, and students.
2. The use of unprotected mobile devices to access or store confidential data is prohibited regardless of whether the equipment is owned or managed by [ORGANIZATION NAME]. Every user of mobile devices must use reasonable care as outlined in this policy to protect against a confidential data breach.
3. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices used to access [ORGANIZATION NAME] systems must be protected by a password. Employees should use a password manager (such as Bitwarden) to protect and manage their [ORGANIZATION NAME] passwords and data. [ORGANIZATION NAME] passwords and data should not be stored on any personal device (including phones, smart watches, laptops, etc) in an unsecured manner that could be accessed by a third party if the device were lost or stolen.
4. Employees understand that their access and/or connection to [ORGANIZATION NAME] networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. [ORGANIZATION NAME] reserves the right to refuse the ability to connect to [ORGANIZATION NAME] infrastructure if it feels such equipment is being used in a way that puts the program systems or data at risk.
5. In the event [ORGANIZATION NAME] confidential data (i.e., email, JusticeServer, CMS, network share) is contained on any personally-owned computer or device that is lost or stolen , it is the employee's responsibility to notify Amanda Revels or Scott Ellis IMMEDIATELY (i.e., no more than one hour after realizing that the equipment is missing) at [[ORGANIZATION NAME EMAIL]](mailto:MAP-IT@lsscm.org) and to their direct email addresses if it is outside of regular work hours.
6. Employee access to company data is limited and automatically enforced based on the employee’s user profile and permissions defined by IT.
7. Employees are required to apply multi-factor authentication to access [ORGANIZATION NAME]’s resources: email, calendars, contacts, documents, case management system, etc.
8. Staff must [enroll the personal devices](https://docs.google.com/document/d/1ytE7edb2AYtpWjzNXaT-9TXDZaUAq5m_3jdvATAzklI/edit#heading=h.bv44na2x78pn) they wish to use for work purposes with Azure Active Directory before downloading Microsoft Office 365 desktop applications and syncing to [ORGANIZATION NAME]’s resources. Instructions for syncing can be found on the [Technology](https://miadvocacyprog.sharepoint.com/sites/hub/SitePages/Technology.aspx?source=https%3A%2F%2Fmiadvocacyprog.sharepoint.com%2Fsites%2Fhub%2FSitePages%2FForms%2FByAuthor.aspx) page of the Hub..
9. Students and volunteers should not sync [ORGANIZATION NAME] data through the OneDrive app, unless there is a compelling work-related need to do so. Documents containing client confidential information that are created and stored in the local drive must be deleted permanently (including from Recycle Bin) as soon as the work is completed. Please also see sections V(F) and (G) below.

1. [ORGANIZATION NAME] will remotely remove all [ORGANIZATION NAME]-related data from an employee’s, student’s, or volunteer’s device when:
   1. The device is lost or stolen,
   2. The employee’s employment is terminated,
   3. IT detects or learns of a data or policy breach, a virus, or similar threat to the security of the company’s data and technology infrastructure.
2. [ORGANIZATION NAME] assumes no responsibility for repair, maintenance, or replacement of personally owned equipment used for work. [ORGANIZATION NAME]-IT may provide general guidance (i.e. working with staff to connect printers or other devices to [ORGANIZATION NAME] equipment) but will not troubleshoot connectivity issues or provide in depth assistance for personally owned equipment.
3. [ORGANIZATION NAME] reserves the right to revoke this privilege if users do not abide by these policies.

1. Limited exceptions to policy may occur due to variations in devices and platforms. Please reach out to [ORGANIZATION NAME]-IT if you think you have circumstances requiring an exception. Only a Director can grant an exception to this policy.

# COMMUNICATION

1. Staff are responsible for checking and responding to voicemail, text, and email messages each work day. If unable to check voicemail or email messages for longer than three days, employees should leave a message to that effect on their voicemail and email.
2. Staff should not make any communication using voicemail, email, or text message that shouldn't be made in a letter or memorandum. Each of these systems presents its own opportunities for humor. However, sometimes things that seem funny at the time appear cruel or otherwise objectionable when received in an email, text, or a voicemail message. Please be aware of this and try to avoid communications that may cause hurt feelings.
3. [ORGANIZATION NAME] email accounts are to be used for [ORGANIZATION NAME]-related correspondence. Employees shall not set up or use mail forwarding from their [ORGANIZATION NAME] email to a personal or any external email address. All [ORGANIZATION NAME] correspondence should be transmitted from and stored in a [ORGANIZATION NAME] email account only.
4. All email accounts should contain the following text below the signature:

|  |
| --- |
| *This electronic communication may be subject to the attorney-client privilege and may contain confidential information. If you are not the intended recipient, any distribution, copying, or disclosure is strictly prohibited. If you have received this communication in error, please notify the sender immediately and delete this copy from your system. Thank you for your cooperation.* |

1. Because texting is not encrypted, email is the preferred method of client communication., All texting with clients should be done directly through our Case Management System (CMS) JusticeServer, RingCentral, or WhatsApp. If the client or [ORGANIZATION NAME] employee needs to text photographs or documents, this can be done via RingCentral; clients may also text photographs or documents via JusticeServer.
2. Some offices may be given shared cell phones for using WhatsApp to obtain signatures and text with clients out of the country; using as a mobile hotspot to connect to the internet when in the field; and for scanning and saving documents/pictures to Sharepoint.
3. Employees should use their [ORGANIZATION NAME]-assigned phone number in all work-related communication (including the setup of a WhatsApp Business account). Employees are not required or expected to use their personal cell phones for work purposes, but if it is unavoidable employees may apply for a phone stipend, per the [ORGANIZATION NAME] Cell Phone policy.
4. Please refer to Section VII below for more information related to sharing confidential information electronically.
5. [ORGANIZATION NAME] currently supports several options for hosting video conferences with clients, co-workers, and partners: Google Meet; Teams; RingCentral; and Zoom (ask [ORGANIZATION NAME]-IT if you need login credentials to host a meeting). Zoom is the recommended platform for trainings and webinars. When recording a training or webinar on any platform, please be conscious of the length of the training, and how long the video needs to be stored. Zoom meetings/webinars should be recorded in the cloud, not locally. Due to limited storage, recordings should be deleted from Zoom when they are no longer needed. If a recording must be retained indefinitely, please reach out to [ORGANIZATION NAME]-IT to discuss where to store it.

# DATA STORAGE

## **File Naming**. All staff should place case-related computer documents in the appropriate common directories and subdirectories. When naming directories, subdirectories, and files, use only letters, numbers, dashes (-), or underscores (\_); do not use brackets, parentheses, periods, or other characters; abbreviate whenever possible because there is a 400 character limit for the total file path name (inclusive of every level of directory and subdirectory needed to access the file). Follow a single scheme in organizing your files in directories and subdirectories, and share your scheme with your manager.

1. **File Storage Organization**. Staff should periodically (at least once a year) clean out their file directories. This can be done by deleting files that are no longer relevant. A better practice for case related files in particular might be creating a subdirectory for noncurrent materials (e. g., G:\PS\OLD\). Any noncurrent documents (e.g., files relating to closed cases) can be moved to this subdirectory where they will be "out of the way", but can be retrieved in the future if they are needed for any reason.

## **Common Directories**. When working in common directories never delete a file unless it was created by or for you, and even then, delete with caution. Before you modify a document not created by or for you, copy it to a new file name in your directory.

## **Backup and Recovery**. Incremental backups are performed each night over WAN and LAN networks to a dedicated backup host; a full backup is performed each weekend. Restore operations are tested at least quarterly. Only IT administrators have access to the backup server. If users notice missing directories or files, please notify Amanda Revels and Scott Ellis promptly at [[ORGANIZATION NAME EMAIL].](mailto:map-it@lsscm.org)

## **Data storage in [ORGANIZATION NAME]’s CMS**. Staff are encouraged to paste or upload important client documents—litigation plans, substantive emails, substantive letters, substantive orders, etc.—into JusticeServer (or any future Case Management System (CMS)).

1. **Encourage working in the cloud**. [ORGANIZATION NAME] encourages working in the cloud whenever possible to avoid downloading confidential client information to your [ORGANIZATION NAME] or personal device. This is critical because if your machine is lost, stolen, or compromised a third party can access confidential client information that has been downloaded. Funders have asked for audit trails when computers have been stolen to ensure that there is no client confidential information available. Additionally, if an employee’s hard drive crashes, there is no way to retrieve anything stored locally or in the downloads folder.
2. **Deleting Sensitive Documents downloaded to [ORGANIZATION NAME] and personal devices**. For the security reasons noted above in V(F), on a monthly basis, , staff should remove files containing confidential client information from their local downloads folder (and other locations not synced to OneDrive or SharePoint). If these local saved files containing confidential client information do not need to be saved to OneDrive or SharePoint, staff should permanently delete them by deleting them and then permanently removing them from the Recycle Bin.

# RESPONSE IN THE EVENT OF A DATA BREACH

## **Definitions**.

## “Data Breach” means the loss of control, compromise, authorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user access or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purposes.

## “Personally Identifying Information (PII)” means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example: first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

## **Actions in the event of a data breach**. [ORGANIZATION NAME] stores personally identifiable information in staff email (currently Gmail), in our case management system (currently JusticeServer), and in our document storage system (currently Office 365/SharePoint). In the event of an actual or imminent breach of personally identifiable information, [ORGANIZATION NAME] IT staff will take all reasonable measures to immediately stop and repair the actual or imminent breach.

1. **Notifications in the event of a data breach**.
2. In the event of a data breach, [ORGANIZATION NAME] will:
   1. notify the affected individual(s) without unreasonable delay, consistent with legitimate needs of law enforcement, or consistent with measures necessary to determine the scope of the breach and to restore the integrity of the data system;
   2. notify law enforcement of the breach as appropriate; and
   3. notify funders as required by the terms and conditions of the funding source.
3. [ORGANIZATION NAME] will include the following information when notifying the affected individual(s):
   1. That the individual’s personal information was acquired or reasonably believed to be acquired by an unauthorized person;
   2. The date or dates of the breach or possible breach;
   3. Those elements of personal information that were likely acquired.
4. [ORGANIZATION NAME] may delay notification if a law enforcement agency requests a delay for criminal investigation purposes. Notification will be made after the law enforcement agency determines that it will not impede the investigation.
5. [ORGANIZATION NAME] will notify the affected individual(s) by one of the following methods:
   1. Written notice to the person’s last known address in [ORGANIZATION NAME]’s records;
   2. Electronic notice consistent with applicable provisions of 15 U.S.C 7001;
   3. Telephonic notice to the last known telephone number in [ORGANIZATION NAME]’s records; or
   4. Substitute notice, such as electronic mail, prominent posting on [https://miadvocacy.org](https://miadvocacy.org/), or notification to applicable local or statewide media, if one of the following conditions exist:
      1. the cost of providing notice would exceed $250,000
      2. the number of individuals to be notified exceeds 500,000; or [ORGANIZATION NAME] has insufficient contact information.

# CONFIDENTIALITY

1. **Passwords**. All employees are issued a username and password for their computer, SharePoint, Case Management System, email, and other miscellaneous systems. These passwords should not be shared and should be kept confidential. Employees should choose passwords that are at least eight characters long and contain a combination of uppercase and lowercase letters, numbers, punctuation marks and other special characters.

Employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack (choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective). Users should avoid dictionary words, common phrases and names. Employees must choose unique passwords for [ORGANIZATION NAME] accounts, and should not use a password that they are already using for a personal account. If the security of a password is in doubt or if it appears that an unauthorized person has logged in to the account, contact Amanda Revels and Scott Ellis IMMEDIATELY at [[ORGANIZATION NAME]-it@lsscm.org](mailto:map-it@lsscm.org) and to their direct email addresses if it is outside of regular work hours[.](mailto:map-it@lsscm.org)

If you have been given an account for a [ORGANIZATION NAME]-assigned password manager (such as Bitwarden), all work-related passwords must be stored there, and shared work passwords should be stored in folders in that password manager and shared with the appropriate employees.

1. **Desktop PIN**. Do not ever change your desktop PIN. If you do have a need to change your desktop PIN, please inform [ORGANIZATION NAME]-IT of your new PIN immediately so they can access your device.
2. **Common Files and Confidential Documents**. Any file on SharePoint may be accessed by anyone with access to that SharePoint Site. Managers have separate Sites for management documents. Staff may not access management Sites without permission. If others find a need to have a Site with restricted user access, please contact [ORGANIZATION NAME]-IT.
3. **[ORGANIZATION NAME]’s Internal Website (Hub)**. The information on the [[ORGANIZATION NAME] internal website](https://miadvocacyprog.sharepoint.com/sites/hub) (the Hub) is [ORGANIZATION NAME] policies and guidance to assist staff in complying with these policies. These sites are password protected and their contents are confidential. The materials on [ORGANIZATION NAME] sites may not be used for any purpose except for [ORGANIZATION NAME] program purposes and they may not be shared outside of [ORGANIZATION NAME] without the prior written approval of a Director of [ORGANIZATION NAME] or MSAS. Violation of this "terms of use" policy could result in employee discipline up to and including discharge.
4. **Email**. Email is confidential. You should not read other people's email without their permission.

# SHARING AND COMMUNICATING CONFIDENTIAL CLIENT INFORMATION

Client information may only be shared electronically after the client has authorized the sharing of their information.

1. **Internal and External Sharing of Confidential Client Information.**
2. Whenever possible, sharing confidential client information internally or externally should be done using [ORGANIZATION NAME]'s secure data sharing platforms.
3. If a [ORGANIZATION NAME] employee is contributing confidential client data to a partner’s platform, use of SharePoint, Teams, or another secure platform is preferred.
4. If a [ORGANIZATION NAME] employee is sharing or communicating information that is not confidential (including non-confidential client information) with internal or external partners, a less-secure platform such as Google Drive may be used. Documents containing client information may not be shared via link or shared with a generic or group email address.
5. Currently, [ORGANIZATION NAME] supports SharePoint and Teams as secure data sharing platforms.
6. External user organizations sharing confidential client information with [ORGANIZATION NAME] must sign a Data Sharing Agreement. [ORGANIZATION NAME] will make template Data Sharing Agreements available.
7. **Internal and External Communication of Confidential Information**.
8. All internal communication (i.e., communication between [ORGANIZATION NAME] employees) including confidential client information must be done using a [ORGANIZATION NAME] email address. Anyone without a [ORGANIZATION NAME] email address is considered an external partner (including casual students or volunteers).
9. All communication (external and internal) that includes confidential client information must be encrypted. Some grants may also require all communication about certain cases or work to be encrypted.
10. All communication (internal and external) including confidential non-client information (including passwords, access codes, bank account or credit card information) must be encrypted.
11. Currently, [ORGANIZATION NAME] supports Virtru and Adobe Sign as encrypted options for email.

C. **Determining What Client Information is Confidential.**

1. “Personally Identifying Information (PII)” means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.
2. Similarly, the decision about what items of PII must remain confidential must be done on a case-by-case basis. Some information must remain confidential such as dates of birth, social security numbers, bank or credit card account numbers, medical records, tax records, drivers’ license or ID numbers, and others. Other information is not as clear. The need for names, addresses, employment/employer information, and many other items of PII to remain confidential depends on the specific circumstances of the individual and the case. Advocates must make these decisions in each instance, and are encouraged to seek guidance from their managers as needed.
3. Advocates should also minimize sharing PII about clients whenever possible. When emailing, consider what information must be shared, and whether it’s possible to communicate without using PII or to share redacted documents when consulting or sharing pleadings.

D. **Use of SharePoint Sites and Teams for Sharing Data**

1. [ORGANIZATION NAME] staff can create SharePoint Sites and Teams groups for the purpose of sharing documents, but these may not be used to **permanently** store client confidential or case information, or as the **primary** place to store such information. Such information should be permanently stored in your office SharePoint sites (which are closed to external users).
2. Sites and Teams **can** be used for collaboration with internal or external partners on projects, and may be used to share confidential information with internal or external partners for the duration of the project. See the [training](https://us02web.zoom.us/rec/play/twwoK3xTm-UOxle9n3FNgO2SELETXh0VAJNftMOOcsmIwQMqnB6TRIgy1waWBlAxT2V2anM06VfSoZn2.iO8ROTIs8gvwWyuQ?startTime=1614350908000&_x_zm_rtaid=ozo5d6y3RhaLGYkOrfamfw.1614521976026.9fc0acdf3df54501f909dedd5b576c03&_x_zm_rhtaid=59) and [slides](https://docs.google.com/presentation/d/16EtQtMJr4XDxT35u7WpFrtcO9e-Jj0DGaNie7BsjlBw/edit?usp=sharing) from [ORGANIZATION NAME] IT for more information on [ORGANIZATION NAME] staff use of Sharepoint Sites.
3. Staff can set up their own Sites or ask [ORGANIZATION NAME] IT for assistance with setup.
4. External users, upon their first login, will be required to register a form of MFA (multi-factor authentication) with [ORGANIZATION NAME] to ensure that no unauthorized access is granted. Please see [Instructions for External Users Accessing [ORGANIZATION NAME] SharePoint Sites and Teams](https://docs.google.com/presentation/u/0/d/1z9gavZVMmr062Q22cVwsV7ma6mvQiR2QJ-Ffkv8y4FA/edit).
5. Duration of sites - External SharePoint sites will be archived by [ORGANIZATION NAME] IT following a period of inactivity of 6 months. After a site is archived it won’t be accessible by members, but it won’t be deleted. However,content that needs to be retained should be moved to permanent, internal SharePoint sites.

# OPEN SOURCE SOFTWARE

[ORGANIZATION NAME] supports the use and creation of open source software as generally in line with our values as a nonprofit poverty law program. We will endeavor to use, support and contribute to open source software in our program whenever feasible.

# TECHNOLOGY PROJECTS AND PURCHASES

[ORGANIZATION NAME]-IT is dedicated to meeting the technology needs of the program in a consistent and efficient manner across the program, and are the program experts in technology solutions.

1. Technology requests should be made in writing to your local office CRP and Managing Attorney, and requests for technology solutions to existing problems should be made to [ORGANIZATION NAME]-IT. Technology decisions are made on a program wide basis in accordance with the technology plan. Before implementing any new technology solution, staff must consult [ORGANIZATION NAME]-IT.
2. Technology purchases. Requests for purchasing any technology equipment (keyboards, cell phones, mice, recording equipment or programs, laptop sleeves, etc.) should not be done without consulting [ORGANIZATION NAME]-IT first. [ORGANIZATION NAME]-IT often has extra equipment available or may make recommendations for specific purchases to ensure compatibility with existing equipment, that high quality equipment is available to staff, and ensure consistency across the program for purposes of future maintenance. [ORGANIZATION NAME]-IT may recommend a particular item to be purchased by the employee’s office through Staples, or may purchase the item and have it shipped to the employee.

# REPORTING AND RESPONDING TO TECHNOLOGY POLICY VIOLATIONS

Any violation of [ORGANIZATION NAME] technology policies should be reported to [[ORGANIZATION NAME EMAIL]](mailto:MAP-IT@lsscm.org) immediately.

Violations of this policy constitute employee misconduct under the [ORGANIZATION NAME] CBA and may result in employee discipline, up to and including discharge. [ORGANIZATION NAME] reserves the right to restrict an individual's access to technology resources as a result of inappropriate use.

Updated July 2023

(signature page below)

AGREEMENT REGARDING TECHNOLOGY POLICY

I have read and I am familiar with the [ORGANIZATION NAME] Technology Policy, and I agree to abide by all terms of these policies. I also understand that [ORGANIZATION NAME]’s Technology Policy may be updated periodically and it is my responsibility to be aware of changes made to the policy by reading emails related to the Technology Policy, and by periodically reviewing it on [ORGANIZATION NAME]’s internal policy website.

This signed acknowledgement must be submitted as part of your onboarding, and will be kept in your Personnel File maintained by [ORGANIZATION NAME] HR.

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dated: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_