Embrace Digital Transformation: Managing Operations

A Detailed Guide on Hardware and Software Tools for the Modern Practitioner

LAW ASSOCIATION OF TRINIDAD & TOBAGO

A GUIDE BY:
THE LAW ASSOCIATION OF TRINIDAD & TOBAGO

PROJECT:
LAW IN THE TIME OF CORONA: EMBRACE DIGITAL TRANSFORMATION: MANAGING OPERATIONS

ELECTRONIC RECORD-KEEPING & STANDARDS

Explore the possibilities of a paperless practice

E-filing presents an opportunity to move to a paperless practice. Since filed documents no longer require the printing of multiple copies we urge practitioners to make efforts to build their capacity to convert physical documents into electronic ones and then thereafter the capability to store these documents in a safe and reliable manner.

Scanners

Practitioner's should consider the limitations of their existing scanners. It is recommended that the practitioner acquire a dedicated scanner to streamline this conversion process. Not only is a dedicated scanner a faster option, it is also more reliable and produces higher quality scans which becomes important given that scanned documents will now be going to the Court and to other Attorneys, and in all cases all parties will be depending on the accuracy and legibility of the documents. The practice directions require documents to be properly oriented, paginated and of an appropriate resolution.

It's imperative to ensure the reliability of scanners used for the processing of large documents. Practitioners should adopt the best practice and combine scanned documents into a single file, with appropriate numbering, ensuring that all pages are correctly oriented without warping and missing areas of content. Scanners 'misfeed', crumple documents, omit pages, scan too dimly, scan too heavily or omit white space incorrectly. All of these are fine tuning issues that will determine your choice.

Portable document scanners (such as the Fujitsu ScanSnap) tend to run smaller and cheaper than desktop scanners. You can find portable scanners as low as $50 US for handheld models and closer to $100 US for those that aren't small enough to be handheld. The more expensive portable scanners inch closer to the $300 US range.

Desktop scanners (such as the Fujitsu 6670) differ from portable scanners in that they're much larger and stationary. Scanning speed and the ability to scan both sides of double-sided images are two other perks of many desktop document scanners. While these scanners tend to be pricier – many advanced models go for well over $400 - $5000 US. Some desktop scanners can also correct errors, for example if you place a document in one way and put the following page in upside down, the machine can recognize the error and still process everything correctly by rotating the page or images.

Read more:
https://www.businessnewsdaily.com/11308-choosing-a-document-scanner.html

Data Storage

After successfully converting your documents into an electronic format they now need to be properly stored. Apart from local storage in your device, it is recommended that all documents be stored with some form of redundancy. This means having backup storage solutions for your data.

To create a simple data backup plan, you need to think about your data structure, real risks, and create backup procedures, which offer simple solutions for the most potential accidents. Typical data threatening situations are accidental deletions, hard disk failures, computer viruses, thefts, fire and flood accidents. Data storage equipment has become more reliable over time, but hard drive failure rate is still around 4.2-4.8% annually.

As possible solutions to these data threats. we recommend Network Attached Storage (NAS) and cloud storage solutions

Network Attached Storage (NAS)

A Network Attached Storage or NAS, is a useful option as it allows for a centralized storage location for all documents and these documents can be accessed remotely. This may require specialized technical assistance to set up a Virtual Private Network (VPN) or install hard drives into enclosures and make appropriate technical adjustments such as setting up Redundant Arrays of Inexpensive Disks or RAID arrays.

This is however a primary storage method and can be seen as a system storage solution rather than a back up data solution. While a NAS may provide some form of back up, this is not their main function. If the NAS is stored in the same physical location this may not accomplish the desired redundancy.

Cloud Storage

Cloud storage can assist with back up storage. It is a cheap and relatively easy solution to employ in your organization and can be seen as a plug and play option. It can be set up quickly on your system and you can set it to automatically backup all documents on your system's local storage. There is a monthly fee attached with this option when you exceed quotas. The costs can add up and should be monitored. The average cost of storage is roughly similar across commercial providers.

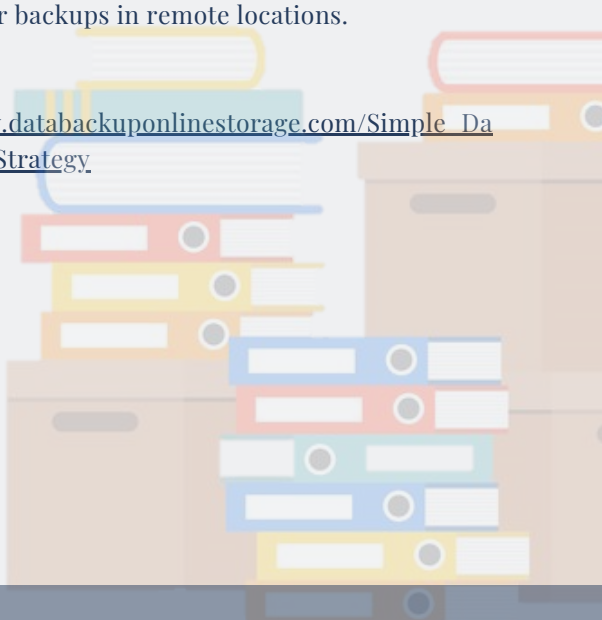
Practitioners should closely consider the privacy policies of these online storage platforms which may use both the Practitioner's data and the client's information either to poll or to disclose to third parties for profit. For example Google's privacy policy says their robots scan your documents (and emails and everything else you create using Google, Chrome, and so on) not only to give you targeted ads, but: "We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services."

Some options of cloud storage to consider here are AWS (Amazon Web Services), One Drive or Dropbox.

Four simple rules for creating your original safe data backup strategy are:

- make copies of your data regularly;
- automate the backup making process;
- save backup copies on different mediums; and
- store your backups in remote locations.

Read more:
https://www.databackuponlinestorage.com/Simple_Data_Backup_Strategy



File organization

Practitioners should establish protocols for the intake of documents. It may be useful to return original documents provided by the client immediately after scanning to reduce the need to hold physical documents. Practitioners should determine what documents are required in active paper files and consider back file conversion. There are commercial players who do this for a fee e.g. Access.

Arrange your files electronically in the same manner and order as if you were organizing a physical filing system. By making conscious decisions about the way documents and folders are arranged and named, it makes sourcing and finding files later on much easier, and will also greatly assist when it comes time for any electronic filing. It ought to be noted that the Judiciary is establishing naming conventions for documents to be uploaded to the e-filing portal. Practitioners may want to await this guide before deciding on the logical organization of files. This will be dealt with in an upcoming guide.

Organization prevents duplication. The tip here is to stop saving documents you may already have. If you focus on proper record keeping then this becomes easier to do. This should be applied to everything from email, file shares, document repositories (on-premise and in the cloud; physical documents and electronic ones), duplicate material, drafts. Thought should be given to legal data retention requirements. While the cost of digital storage looks cheap on its face, the total cost of ownership (TCO) should be carefully monitored

DATA CONFIDENTIALITY & PROTECTION

Mitigate against the risks of electronic record-keeping

While there are many benefits to electronic record keeping, we emphasize that there are risks involved with having electronic record keeping as the primary form of information storage. One major risk arises from your duty to manage and protect the distribution and access to these files.

When a document is converted into an electronic form it becomes susceptible to data breaches. This may come either from an individual with physical access to the data or system or from external sources such as hacking, malware, spyware and other malicious software. Steps should be taken to physically secure computers. Networks should also be protected. Practitioners should consider the security of their networks and seek specialist assistance where necessary and consider establishing role-based access.

Read More:
https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

Even if your organization is small, you need to think about which employees need and should have access to what information. (Your confidential files, for example, shouldn't be accessible to everyone, and access to invoicing and banking information must be limited. Practitioners should perform a data risk assessment and familiarize themselves with possible dangers such as Man In the Middle Attacks (MITM) and spoofing and use the most secure online resources available. Electronic files should be managed with the same care as physical files to ensure compliance with ethical obligations. Sometimes data breaches can be caused due to the carelessness of just one employee losing a device which is subsequently compromised.

THE NEW PAPER-LESS OFFICE

Enter the new age of the paperless office

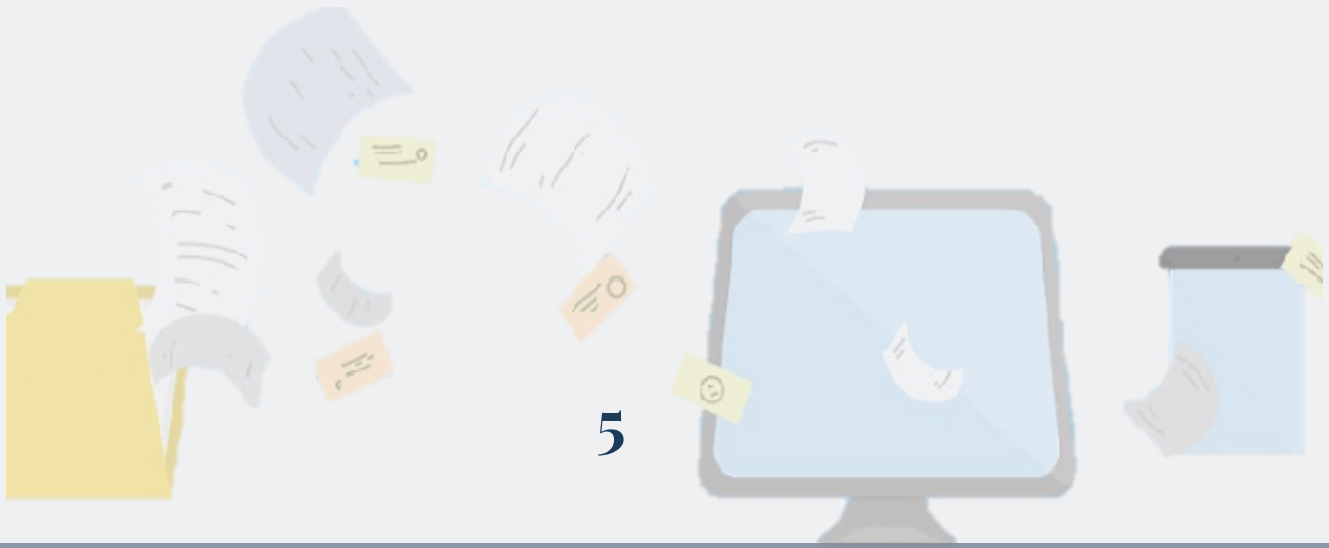
Staff must be properly trained in the use of virtual/paperless office management so that tasks can be effectively completed under the new Practice Directions, be they filing or clerical work. Computer systems should be up to specification so as to allow ease of video conferencing and running PDF software. Practitioners should ensure that their computers meet the basic specifications. Older computers can sometimes make even relatively simple tasks such as compiling multiple PDF documents a very time consuming task.

Decisions will have to be taken as to what documentation and information should be kept and what should be discarded, given that there would be a transitory period. We understand that it is difficult for practitioners to take their entire practices virtual immediately. We advise that members take all necessary steps to ensure that they are in the best position to file electronically, and this can mean making sure that key documents are scanned and stored electronically ahead of time.

The introduction of productivity and communication apps such as Slack, Webex and Trello should be used to delegate tasks and keep abreast of workflow production while allowing members of the team to communicate. Consider using practise management software such as Clio, Cicero and BlueStylus which allows for the virtual management of your legal practise and integrates calendaring, timelines and task updates. The cost of these applications should be rationalized.

Where a face to face meeting is necessary consider using apps like Microsoft Teams, Webex or Teamviewer which are virtual meeting spaces that can be used amongst a legal team to coordinate workflow and productivity. Collaboration Applications and Software such as Microsoft Office Online, Microsoft Office 365 and Google Documents may assist in quicker revisions of documents. Training support staff in the use of these applications and proper system specifications are both integral for the deployment of the paperless office.

Read More:
https://docs.microsoft.com/en-us/azure/role-based-access-control/overview



SIGN ELECTRONICALLY

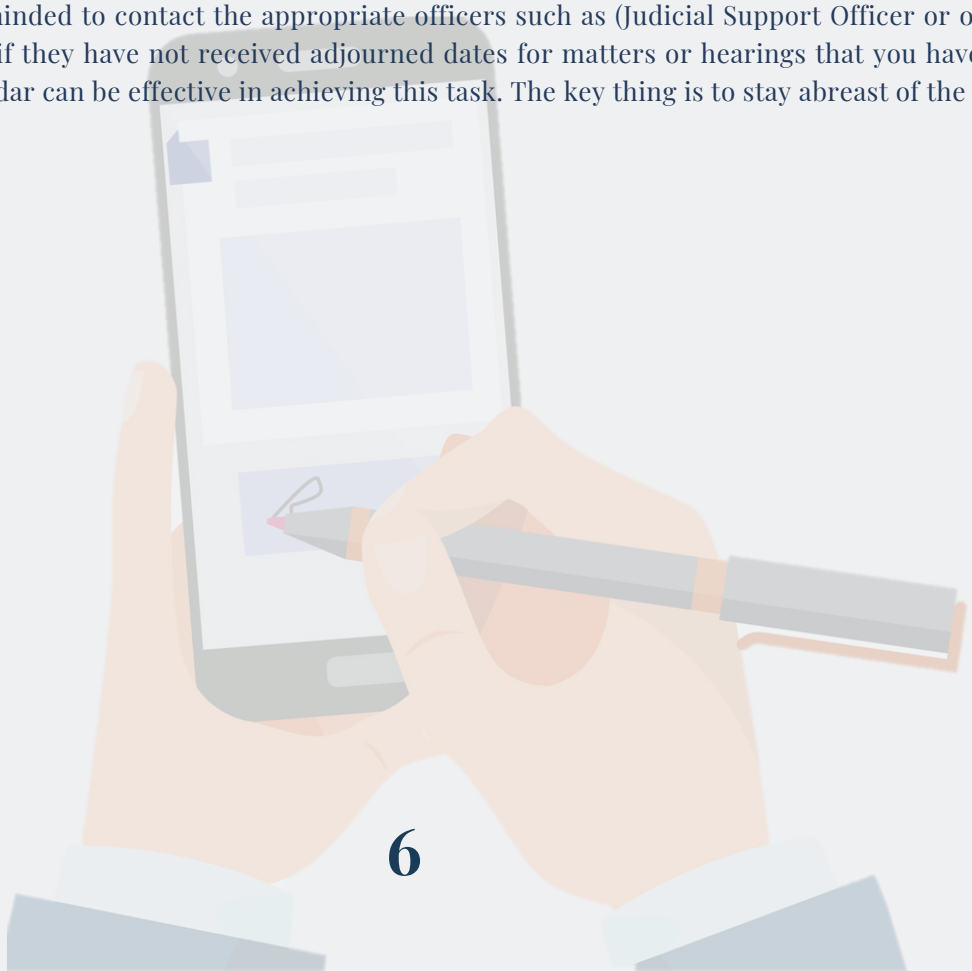
A digital signature as unique as your own

DocuSign, PandaDoc and Formstack Sign are all ways to sign documents electronically. Software to sign electronically and its validity is more than just adding in a digital signature to a document. The use of electronic signature software allows the signature being attached to be encoded and as unique as a physical signature. In most cases digital signature software can be more secure than a physical signature as it allows persons viewing the document to see evidence of even the most minor tampering with the document and signature. In these times of social distancing a free electronic signature application can do much to safeguard against forgeries and will be extremely useful and necessary for electronic filing.

CALENDARING

Keep up-to-date with all your matters

Practitioners are reminded to contact the appropriate officers such as (Judicial Support Officer or other similar administrative staff) if they have not received adjourned dates for matters or hearings that you have during the period. Google Calendar can be effective in achieving this task. The key thing is to stay abreast of the dates.



BANDWIDTH

Stream faster than ever before

What is bandwidth? When streaming out to the internet, you are consuming upload bandwidth. Examples of uploading include attaching a file to an e-mail, saving a file to Cloud storage, or publishing a live stream. As with download bandwidth, upload bandwidth has a set rate (i.e. "5 Mb/s up") as dictated by your internet service provider (ISP). Download bandwidth limits are also generally higher than upload limits (e.g. "15 Mb/s down and 5 Mb/s up"). It is essential to know your network's upload speed because this rate enables (and also limits) the quality of your outgoing streams. Many ISP's advertise upload and download bandwidth in terms of a maximum speed.

For example, an internet package might be advertised as "Up to 10 Mb/s up and 30 Mb/s down!". This particular "up to" phrasing is used because Internet speeds can vary. If using a cable network, for example, you're sharing Internet with other cable users within a geographical area, so your bandwidth may slow during "peak" periods of Internet activity during the day. Ensure you always have enough bandwidth for streaming your broadcast—plus more. This extra "headroom" acts as a buffer to account for any changes to your network. Upload bandwidth can be affected by all forms of user activity on your network, such as Internet uploads, or Voice over IP (VOiP) communication such as Whats App calls.

Read more: https://www.epiphan.com/blog/bandwidth-for-streaming/

Before engaging in electronic hearings with the Judiciary, parties are required to conduct tests. One of these tests is an upload speed test. Practitioners are reminded that bandwidth can be consumed by other devices currently on the network and what those devices are currently doing on the network. For example if you have an electronic hearing care should be taken to reduce to the numbers of persons actively using the network for network intensive tasks for example video content or downloading large files as this could disrupt the streaming video link.

Video conferencing requires a lot of bandwidth and multiple devices overloading the network can directly hamper not only video quality but also audio quality as well. For this reason if hearings are being done at home or at the office we advise that adequate steps are taken to ensure that the bandwidth is not compromised in the manner mentioned above.

VIDEO CONFERENCING

Change the way you communicate

Practitioners should consider video conferencing hardware. There are many commercially available solutions from companies such as Cisco, Polycom, Avaya etc. They should consider that there are consumer grade solutions and commercial solutions. The spend on this area should be rationalized. These items can sometimes integrate with a practitioner's telephone systems to allow for seamless transition from mobile, to landline, to online communications both with and without video (Unified Communication)

PRACTICE RESOURCES

Optimize your practice with these useful resources

PDF Optimization with Adobe

Practitioner's should consider useful guidance from Adobe and other PDF software on-
i. Optimizing PDFs to reduce file size - https://helpx.adobe.com/acrobat/using/optimizing-pdfs-acrobat-pro.html
ii. Hyperlinking - https://blogs.adobe.com/acrolaw/2010/04/creating-hyperlinks-in-adobe-acrobat/
iii. Combining files into a single pdf - https://acrobat.adobe.com/ca/en/acrobat/how-to/merge-combine-pdf-files-online.html
iv. Practitioners should also familarize themselves with learning how to edit PDFs natively by adding text, inserting Bates Numbering, bookmarking, and rotating and resizing pages.

Online Legal Resources

Practitioners should be aware that there are multiple online resources to which can greatly assist in research and drafting of documents. They may require a subscription and payment of the associated fees. Common examples include:

- BAILII (British and Irish Legal Information Institute)
- JustisOne
- Westlaw
- LexisNexis

Bring Your Own Device Policy (BYOD)

Practitioners that exist on networks with many participants could consider establishing a bring your own device policy. A BYOD policy permits employees to purchase and use devices (e.g. computers, smartphones and tablets) of their choosing at work for their convenience subject to agreeing to be bound by terms and conditions of device use while attached to the network. This would include such considerations as establishing a strong password scheme for access to the network and network resources.

If persons access the network using shared devices, these passwords can perhaps become compromised due to negligent physical access. This can be prevented by enforcing a remote data wiping policy which would provide that the employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure. Such a policy would also restrict misuse of confidential information and utilizing personal devices for the storage and transmission of illicit media.

Network security primers

Basic network security primers should be considered such as encrypted passwords with 2 factor authentication, meaning the access is verified not only by having the password but also by way of an external means such as a text message or an email to a designated account.

Read more:
https://www.sans.org/network-security

https://searchsecurity.techtarget.com/definition/two-factor-authentication

A GUIDE BY:
THE LAW ASSOCIATION OF TRINIDAD & TOBAGO

PROJECT:
LAW IN THE TIME OF CORONA: EMBRACE DIGITAL TRANSFORMATION: MANAGING OPERATIONS

LAW ASSOCIATION OF TRINIDAD & TOBAGO

BACKGROUND

The Law Association of Trinidad and Tobago is committed to assisting all legal professionals as far as reasonably practicable. This brochure is produced by our Information Technology Committee and is one of a series containing guidance which we hope will assist legal professionals in continuing business operations during the Pandemic period.

We hope it will be useful to you. If you have any questions, comments and/or suggestions on how to improve the information contained in this brochure, please feel free to contact the IT Committee
admin@lawassociationtt.com

CONTACT DETAILS

Address: 2nd Floor, #95-97 Frederick Street,
Port of Spain, Trinidad, W.I.
Phone: 1-(868)-225-8715-7
Email: admin@lawassociationtt.com
Website: https://lawassociationtt.com/contact-us/