ASA MEDICAL GROUP

**Storing and transferring work data policy**

**Created July 18, reviewed June 2022**

Employees at ASA Medical Group are given a variety of resources to do their jobs efficiently and effectively. But it’s important that these resources are carefully guarded.

Storing, transferring and sharing company information comes with risks. It can result in data breaches (in which company data is released to people outside of the organization or employees of the organization who haven’t been granted access to it), data theft (in which hackers steal information for financial gain or to gather intelligence) and misplaced data (in which original files become lost or unavailable).

The purpose of this policy is to ensure that data is kept available only to current employees of The Sandringham Practice who have been pre-approved to possess it.

**1. Email**

All data sent over email (as an attachment or in an email text) should be considered sensitive and protected as such. Never send work documents or information to someone outside of the company unless it has been cleared by a manager and IT. *This includes forwarding company emails to your own personal email account.*

Note: Not all users within ASA Medical Group have access to the same information. Before sending data or files to a co-worker in an email, check with your manager to be sure the recipient is allowed to have access to it.

**2. Cloud storage and cloud applications**

We appreciate that workers may sometimes need access to work outside of the office from home, mobile devices or company equipment on the road. However, *work information should never be stored or shared to personal cloud accounts or applications, such as iCloud, Google Drive, Box, Dropbox, Microsoft OneDrive, etc.*

Should you need to store or backup data online, IT has approved the following services for doing so:

* The shared practice folder, office manager or senior manager folder

If you would like guidance on how to use these services, IT would be happy to assist. And if you have any questions on whether a service is appropriate to use, ask IT *before* using it.

[Note: You may also want to provide the steps needed for getting approval for a new cloud service if applicable.

**3. Physical storage devices**

Storing work data on physical devices, including but not limited to USB drives, memory cards, CD or external hard drives, must be pre-approved by IT.

* Employees of The Sandringham practicemust only use devices provided by the company unless otherwise given permission.
* NEVER use or even plug in a USB drive that you have found or been given as a promotional item. These devices may contain hidden malware or viruses.
* Lost or stolen devices must be reported to IT and a manager immediately to help ensure their safe return and prevent a data leak.

**4. Social media for work data**

Work data or information must never be shared over social media accounts such as Facebook, LinkedIn, Google Plus, etc. Never respond to posts from patient or posts about the practice or staff.

**5. Encryption**

While encrypting data may not prevent a data breach, it can help ensure that if information falls into the wrong hands it can’t be read or used. The Sandringham Practice requires the following types of information to be encrypted: SARS, occupational health forms If information is required to be encrypted, it must be protected by [a strong password](http://www.itmanagerdaily.com/password-policy-template/) and should never be copied or shared in a way that would make it available outside of the encryption process.

*Whenever you have any doubt or questions on data transfers, contact IT before doing anything else. We will be happy to help you and guide you through the process.*