Backup your important data

AAPi
AUSTRALIAN ASSOCIATION
of PSYCHOLOGISTS INC

AAPi member support is often asked questions about file storage. It is important to remember that all electronic files need to be kept secure and backed up.

Valuable data such as client files, emails, billing history and text messages can be lost instantly, so it is important to back it up regularly before it's too late.

Our devices hold a great deal of our data, but if your device is damaged, lost, or destroyed, your data may be lost. Whether it's because of hardware failure, theft, accidental damage, or your device is infected with a virus, recovering data can be expensive and sometimes even impossible. That is why it is so important to schedule regular backups, so you can restore your data if something goes wrong.

How do I backup my data?

Backing up is different for everyone. Some simple steps you can take are:

- **Choose what data to include in your backup** – Think about what you want to keep safe. It may be your most important files, or it may be an entire system.
- **Decide how to back up your data** – There are different ways. You could use a cloud backup service, an external storage device, or a combination.
- If you use an online client management system, **check how often your data is automatically backed up** and how you would access these backups if needed.
- **Maintain a regular backup routine** – Decide whether it is daily, weekly or monthly.
- **Set automatic backups** – It will reduce the burden of manually creating them each time.
- **Secure your backups** – They contain personal or sensitive information. You should protect them like any other copy of your data. All data backup of Australian Psychologists needs to comply with Australian Privacy Principles and be kept within Australia, encrypted and password protected so that it is secure from misuse, interference and loss, and from unauthorised access, modification or disclosure. Steps you could take to secure your backups include disconnecting your backup when not in use, keeping an offline backup like a portable hard drive, storing your backup at an offsite location, storing in a locked cabinet or filing cabinet, using multi-factor authentication, and using strong passwords. For more information about how to comply with the Privacy Principles, please see the Office of the Australian Information Commissioner.
- **Check that your backups work** – testing that you can restore your data will give you peace of mind.

Keeping your devices and data backed up is essential. To learn more about the simple steps you can take, visit cyber.gov.au/backups.

Take the time today to review your practice policies about client data storage and do a backup of your clients' electronic data.