Backing Up Your Data

A Practical Guide to Protecting Your Information
LaFaries Mortimer LLC

Why Backups Matter

Data loss does not only happen to large corporations. Individuals, small businesses, ministries, and organizations lose critical information every day due to hardware failure, accidental deletion, cyberattacks, theft, and natural disasters. Backups ensure that your work, records, photos, financial data, and intellectual property are recoverable when something goes wrong.

What Should Be Backed Up

• Business documents and contracts
• Financial records and tax files
• Client and member data
• Emails and attachments
• Photos, media, and creative work
• System settings and configurations

Types of Backups

Local Backups: External hard drives or USB storage kept physically with you. These are fast and convenient but vulnerable to theft, fire, or damage.

Cloud Backups: Secure online storage that automatically syncs your data. Cloud backups protect against physical loss and allow recovery from anywhere.

Hybrid Backups: A combination of local and cloud backups, offering the strongest protection.

Best Practices for Reliable Backups

• Follow the 3-2-1 rule: 3 copies of your data, on 2 different types of storage, with 1 off-site copy.
• Automate backups whenever possible to reduce human error.
• Encrypt sensitive backups to protect confidential information.
• Test your backups regularly to confirm they can be restored.
• Document your backup process so others can follow it if needed.

How LAAP™ Helps

The LAAP™ System provides structured document storage, guided organization, and secure record management to support proper backup practices. By keeping files organized and documented, recovery becomes faster and less stressful.