

Digital Assets & Online Accounts

Your digital life is more complicated than you think.

You probably have dozens of online accounts. Email. Social media. Cloud storage. Banking apps. Streaming services. Online shopping accounts. Loyalty programs. Newsletters you signed up for in 2014.

When you die, your executor will usually need to deal with your online life. That can mean:

- Access your email to notify contacts and close accounts
- Recover important files from cloud storage
- Close or memorialise your social media accounts
- Cancel subscriptions so your estate isn't charged monthly fees forever
- Access photos, documents, and other digital assets your family might want

But here's the problem: most of these accounts are password-protected, and many have two-factor authentication (2FA) that sends a code to your phone. If your executor can't unlock your phone or access your email, they're locked out. Where a provider has an official process for a deceased person's account, that is usually the safest way in. Logging in directly with someone else's password can break the provider's rules, so for anything valuable or complex it is worth getting advice first.

This section helps you document your digital life so your executor can actually access it.

How should you store passwords?

Do NOT write your actual passwords in this book. If this book is lost or stolen, someone could access your entire digital life.

Instead, use one of these methods:

Password manager. Apps like 1Password, Bitwarden, or LastPass store all your passwords securely. Your executor just needs the master password to access everything. This is the best option.

Encrypted file. Store your passwords in an encrypted file on your computer or in cloud storage. Give your executor the decryption key (stored separately from this book).

With your solicitor. Some solicitors will store a sealed envelope with your passwords. Your executor can collect it after you die.

In a safe. Write your passwords on paper and store them in a fireproof safe at home. Tell your executor the combination.

Whatever method you choose, note it here so your executor knows where to find your passwords. Keep in mind that having a password doesn't always give legal authority to use an account, so for important accounts (banking, crypto, business) your executor may still need to go through the provider's process or get advice on what they're allowed to do.

What about two-factor authentication (2FA)?

Two-factor authentication is great for security, but it's a nightmare for executors.

If your accounts use 2FA, your executor will need:

- Access to your phone (to receive SMS codes)
- Access to your authenticator app (Google Authenticator, Microsoft Authenticator, etc.)
- Access to your email (if 2FA codes are sent there)

Make sure your executor can unlock your phone. If your phone is locked with a PIN, fingerprint, or face recognition, they'll be locked out unless you share access details.

WHY THIS MATTERS

Your executor can't close your email account, access your cloud storage, or cancel your subscriptions if they can't log in.

Without access to your digital accounts, your family might lose precious photos, important documents, or financial records. And your estate might keep paying for subscriptions you're no longer using.

Document your digital life. It's worth it.

Your Digital Assets & Online Accounts

The keys to your digital life: where passwords live, and what to do with each account.

PASSWORD STORAGE

Note WHERE your passwords are kept. Never write the master password in this book.

WHERE PASSWORDS ARE STORED

PASSWORD MANAGER (WHICH)

MASTER PASSWORD STORED AT

SMARTPHONE

PHONE TYPE

PHONE NUMBER

HOW IT'S LOCKED

PIN / PASSWORD STORED AT

TWO-FACTOR AUTHENTICATION SET UP?

COMPUTER / LAPTOP

COMPUTER TYPE

LOGIN PASSWORD STORED AT

IMPORTANT FILES / FOLDERS

BACKED UP? (WHERE)

Your Digital Assets & Online Accounts (cont.)

TABLET / IPAD

DEVICE TYPE

LOGIN PASSWORD STORED AT

EMAIL ACCOUNT 1

EMAIL ADDRESS

PROVIDER

PASSWORD STORED AT

WHAT SHOULD HAPPEN TO IT

EMAIL ACCOUNT 2

EMAIL ADDRESS

PROVIDER

PASSWORD STORED AT

WHAT SHOULD HAPPEN TO IT

CLOUD STORAGE 1

SERVICE

ACCOUNT EMAIL

PASSWORD STORED AT

WHAT SHOULD HAPPEN TO FILES

Your Digital Assets & Online Accounts (cont.)

CLOUD STORAGE 2

SERVICE	ACCOUNT EMAIL
PASSWORD STORED AT	WHAT SHOULD HAPPEN TO FILES

SOCIAL MEDIA (SEE ALSO THE SOCIAL MEDIA CHAPTER)

FACEBOOK + WHAT HAPPENS	INSTAGRAM + WHAT HAPPENS
LINKEDIN + WHAT HAPPENS	TWITTER / X + WHAT HAPPENS

ONLINE BANKING & FINANCIAL (LOCATION ONLY)

Do NOT write banking logins here. Note only where the login details are kept.

ONLINE BANKING 1 + LOGIN STORED AT	ONLINE BANKING 2 + LOGIN STORED AT
INVESTMENT PLATFORM + LOGIN STORED AT	CRYPTO EXCHANGE + LOGIN STORED AT

Your Digital Assets & Online Accounts (cont.)

SUBSCRIPTIONS (SEE ALSO THE MEMBERSHIPS CHAPTER)

Your executor should check bank statements for recurring charges to cancel.

STREAMING SERVICES

SOFTWARE / APPS

OTHER SUBSCRIPTIONS

PHOTOS & PERSONAL FILES

WHERE STORED

WHAT EXECUTOR SHOULD DO

NOTES: ANYTHING ELSE ABOUT YOUR DIGITAL ASSETS