

Devices & Access

Your devices hold your entire digital life.

Your phone has your emails, messages, photos, banking apps, and two-factor authentication codes. Your computer has files, documents, and years of work. Your tablet might have books, notes, and important PDFs.

When you die, your executor needs to access these devices to:

- Retrieve important files and photos
- Close online accounts
- Notify contacts
- Cancel subscriptions
- Access two-factor authentication codes

But most devices are locked with PINs, passwords, fingerprints, or face recognition. If your executor can't unlock them, they're locked out of your entire digital life.

This section helps your executor access your devices and recover what matters.

The problem with device security:

Modern devices are designed to be secure. That's great while you're alive. But when you die, that security becomes a problem.

If your phone is locked with Face ID and no one knows your PIN, your executor can't get in. Apple won't unlock it. Google won't unlock it. The device is effectively a brick.

Same with computers. If your laptop is password-protected and encrypted, and no one has the password, the data is gone forever.

You need to give your executor a way in.

How to give your executor access:

Here are your options:

Write down device PINs and passwords and store them securely. In a safe. With your lawyer. In a password manager. Just not in this book.

Add a trusted contact to your Apple ID or Google account. Apple allows you to designate a Legacy Contact who can access your iCloud data after you die. Google has an Inactive Account Manager that lets you specify what happens to your account if you stop using it.

Make sure your executor can unlock at least one device. If they can unlock your phone, they can access your email and 2FA codes, which gets them into everything else.

Tell your executor where your devices are. If you have a laptop in a drawer, a tablet in the study, or an old phone in storage, they need to know where to find them.

WHY THIS MATTERS

Your executor can't do their job if they can't access your devices.

They can't notify contacts. They can't close accounts. They can't recover photos. They can't access banking apps. They're stuck.

By documenting your devices and providing access, you're giving them the keys to your digital life.

Your Devices & Access

How to get into your devices and accounts, so nothing is locked away forever.

SMARTPHONE

Note where the PIN/password is stored, never the code itself.

PHONE TYPE

PHONE NUMBER

HOW IT'S LOCKED

PIN / PASSWORD STORED AT

CLOUD ACCOUNT (ICLOUD / GOOGLE)

CLOUD ACCOUNT EMAIL

CLOUD PASSWORD STORED AT

LEGACY / INACTIVE CONTACT SET UP?

IMPORTANT APPS

WHERE PHONE IS KEPT

COMPUTER / LAPTOP

COMPUTER TYPE

LOGIN USERNAME

LOGIN PASSWORD STORED AT

HARD DRIVE ENCRYPTED?

DECRYPTION KEY STORED AT

IMPORTANT FILES / FOLDERS

Your Devices & Access (cont.)

BACKED UP? (WHERE)

WHERE COMPUTER IS KEPT

TABLET / IPAD

DEVICE TYPE

LOGIN PASSWORD STORED AT

IMPORTANT FILES OR APPS

WHERE IT'S KEPT

EXTERNAL DRIVE 1

TYPE

WHERE STORED

WHAT'S ON IT

PASSWORD-PROTECTED? (STORED AT)

EXTERNAL DRIVE 2

TYPE

WHERE STORED

WHAT'S ON IT

PASSWORD-PROTECTED? (STORED AT)

Your Devices & Access (cont.)

CLOUD STORAGE ACCESS

ICLOUD EMAIL + STORED AT

GOOGLE DRIVE EMAIL + STORED AT

DROPBOX EMAIL + STORED AT

ONEDRIVE EMAIL + STORED AT

SMART HOME DEVICES

SMART SPEAKER / ASSISTANT

SMART SECURITY SYSTEM

SECURITY LOGIN STORED AT

OTHER SMART DEVICES

OLD DEVICES IN STORAGE

Check old devices for photos, files or account access before disposing of them.

DEVICE 1: TYPE & WHERE

WHAT MIGHT BE ON IT

DEVICE 2: TYPE & WHERE

WHAT MIGHT BE ON IT

YOUR WISHES FOR YOUR DIGITAL DATA

PHOTOS

PERSONAL FILES / DOCUMENTS

Your Devices & Access (cont.)

EMAILS AND MESSAGES

WORK FILES

NOTES: ANYTHING ELSE ABOUT DEVICES AND ACCESS