Digital Estate Planning Guide

[Death & The Digital Estate Community Group](https://github.com/openid/death-and-the-digital-estate/), [The OpenID Foundation](https://openid.net/)

# 1. Overview

Have you ever considered your *digital estate*? You might be surprised to know that if you use any online services - and even if you don’t! - you have a digital estate. What is in your digital estate? All of the data about you, including your:

* Images (photos, drawings, digital imagery)
* Video & Audio recordings
* Files (documents, spreadsheets, presentations) stored locally and in the cloud
* Social media accounts
* Browsing history
* Financial services (banks, brokerages, insurance, cryptocurrencies)
* Loyalty cards
* Utilities
* Credentials to login to online services

We often don’t think about our digital footprint and what will happen to that data when we become incapacitated - temporarily or permanently - or when we die. The guide below is to encourage you to think about your digital estate. The choices you make *today* can impact how your digital estate is maintained and how your digital services can be managed on your behalf when you are no longer able to do so.

The good news is that you *can* start actively managing your digital estate and develop mechanisms for your trusted friends and loved ones to manage it for you when the time comes. Following the guidance below, you’ll be able to identify the assets in your digital estate, identify how they are accessed, and how they will be accessed and managed by your estate.

# 2. Getting Started

## 2.1 What Is Your Digital Estate?

How do you define the extent of your digital estate? Does it include all digital assets, including those on your phone, computer, tablet, social media,and cloud storage for files, email, calendars, photos, etc? What about other digital data, including local backups, external hard drives and memory cards (e.g. SD cards for cameras)?

Defining your digital estate is an *individual exercise* - no two people have the same set of assets in their digital estate. Although many digital estates will share common items, such as social media accounts, the contents of *your* digital estate unique. Therefore, we can define broad categories of data that are commonly found in a digital estate to guide discovery and documentation of your digital estate. The estate owner is the only person who can identify all components of their digital estate, ensuring complete coverage.

Second, digital estates may have different components represented by the personas an individual presents themselves as. For example, one of the authors of this document has the following personas that need to be considered: individual, parent of minor children, board advisor to multiple start up companies, OpenID Foundation member and co-chair of a working group, and employee. Other personas might include legal representative of others via power of attorney, <more examples…?> Each of these personas may have components of a digital estate that should be considered.

For example, as an individual this author has a GitHub account that is used to store code and other digital artifacts related to personal projects. In his persona as a member of the OpenID Foundation and co-chair of the Death & The Digital Estate Community Group, he manages the group’s GitHub wiki pages. When considering his digital estate, it is important the he distinguishes how the estate is managed for each persona. Personal projects in GitHub may be managed by his immediate family while Death & The Digital Estate assets should be transferred to management by the OpenID Foundation.

## 2.2 Why Do You Need to Plan for It?

Just like a complete estate plan requires fiduciary, legal, and healthcare powers of attorney to arrange for a time when you lose the capacity to access and manage your affairs, the modern world requires the same for your digital resources. Failure to do so may result in your beneficiaries, loved ones, and trusted individuals gaining access, and permanent loss of valuable personal history or the ability for others to carry out your wishes. Even with a plan, laws and privacy rights make this a tricky journey. Without a digital estate plan, those who are working on your behalf will be crippled as they start the journey to execute your desires.

## 2.3 What Can Go Wrong Without a Plan?

# 3. How to Plan Your Digital Estate

## 3.1 Identifying Your Digital Assets

For many people, the first place they can begin to assess the scope of their digital assets is through their mobile phone. Users of Apple’s iOS or Google’s Android phones likely have photos and videos stored on their phones, and one or more cloud services. The apps installed on the phone provide a map to where digital data may be stored, including password managers (more on this below!), social media, file storage, media storage (audio, video, photos), financial accounts, and more. In addition to applications on the phone, review the bookmarks in your browser to identify other services that you use. Of course, any data stored on the phone or automatically backed up to the cloud should be considered, including text messages (e.g. SMS, iMessage, Signal, What’s App), and voicemail messages.

This exercise can be repeated for all of the devices that the user owns, including tablets, laptops, streaming devices (e.g. AppleTV, Roku, etc.), cameras (still & video), and media storage (e.g. CDs, DVDs, hard drives, memory cards for cameras, etc.)

Another rich source of information is your email! Review old emails to identify other services that send you email, this includes your bank, brokerage accounts, crypto accounts, insurance companies, healthcare providers, and other businesses that you communicate with.

As we move through 2025 and 2026, the authors expect that we’ll see increased use of password managers (credential managers) due to the growth of passkeys in the consumer market. If you use a credential manager, e.g. 1Password, Dashlane, Apple Passwords, Google Password Manager, etc., it can serve as a critical repository of information about your digital assets, including the credentials used to access them.

Each of these steps can be used to discover the scope of your digital assets, enabling you to determine how to manage them as part of your digital estate. However, there are likely to be lesser used, or no longer used, assets that escape categorization through this mechanism. Unfortunately, there are no comprehensive tools that enable discovery and categorization of these assets today.

Below, you will find a list of common assets in a digital estate, prioritized by their importance for management by the heirs of your digital assets. As noted above, this list is not exhaustive, it is up to each individual to identify and document assets that are not found on this list as part of their digital estate planning process.

### 3.1.1 High-Priority Accounts

* Primary email accounts
* Apple iCloud / Google account
* Password managers (1Password, Bitwarden, etc.)

### 3.1.2 Critical Infrastructure

* Utilities (electric, water, internet, mobile phone)
* ISP and home network credentials

### 3.1.3 Financial and Cryptographic Assets

* Bank and investment accounts
* Home, life, auto, umbrella, and disability insurance accounts
* Crypto wallets and exchanges
* Social security, Medicare/Medicaid, and other government accounts

### 3.1.4 Media and Personal Archives

* Cloud photo & video libraries (Google Photos, Apple Photos, Flickr, etc)
* All other media (audio, documents, spreadsheets, art, etc.) stored digitally (e.g. iCloud, DropBox, Google Docs, Microsoft Entra)
* Code and other artifacts (GitHub, GitLab)
* AI Agents (ChatGPT, OpenAI)

### 3.1.5 Local and Device-Based Data. Victor Lu

Local and device-based data represent a critical but often overlooked component of a person's digital estate. Unlike cloud services that may provide recovery mechanisms or centralized access, data stored directly on physical devices is highly susceptible to loss, decay, or inaccessibility—especially when no backup mechanisms are in place.

* Unbacked-up device storage

#### 

A significant portion of personal and professional digital content remains confined to local storage on devices such as laptops, desktops, external hard drives, or mobile phones. When these devices are not regularly backed up to a secure and redundant system (e.g., cloud storage, network-attached storage), the risk of permanent data loss becomes high in the event of device failure, theft, or user death. From a digital estate perspective, this creates a "black hole" in the continuity of information transfer, leaving executors and heirs without access to potentially valuable or sentimental content.

Digital estate plans should explicitly inventory all such devices, specify whether their contents are backed up elsewhere, and outline steps for secure access posthumously. This may include encryption keys, passcodes, or physical custody instructions.

* Important files on local devices

Files of considerable importance—such as tax documents, unpublished manuscripts, medical records, password vaults, or original creative work—are frequently stored locally, either by default or out of habit. Unlike emails or social media content which reside on third-party servers, these files have no inherent recoverability unless proactively archived or mirrored to external systems.

An effective digital estate plan must account for these isolated data assets. Individuals should flag directories or file types of high relevance, ensure they are backed up or migrated to managed storage, and document access procedures for their digital executor. At minimum, metadata such as device names, user credentials, and physical locations should be recorded in an estate-accessible inventory.

### 3.1.6 Home Networks and IoT Devices

* WiFi credentials
* Smart home configurations (lights, solar, etc.)

### 3.1.6 Health & Medical Care

* Healthcare provider accounts

# 4. Building the Plan

## 4.1 Creating Your Asset Inventory

***N.B.***  *This should probably be a companion spreadsheet*

* Name
* URL or Identifier
* Username
* Credential storage location
* Second-factor method(s)
* Linked credentials
* Legacy contact info
* Account policy for takeover
* Preferred handling instructions

# 5. Choosing a Digital Estate Manager

## 5.1 Who Should Manage It? (miki b)

Choosing the right person (or people) to manage a person’s digital identity and assets in the event of death or incapacitation is crucial. Ideally, it would be someone who understands technology or can follow instructions, as well as be trustworthy, sympathetic and sensitive to the person’s wishes.

It may be worthwhile having more than one person at least aware of the management if not assisting in the preparation. This would avoid anything being missed, incorrectly recorded / conveyed, or possibilities of issues like elderly abuse.

Below are some options with pros and cons for each:

### 5.1.1 Trusted Family Member or Friend

*Example:* You designate your adult daughter, who knows your digital habits and is familiar with your email and online banking, as your digital steward in a written statement.

Pros:

* Personally knows your values and likely to honor your wishes.
* Easier to communicate your intentions informally during your lifetime.
* May already be familiar with your digital habits and devices.

Cons:

* May not have sufficient technical knowledge.
* Emotional burden during a time of grief.
* Potential for family conflicts or differing interpretations of your wishes.

### 5.1.2 Professional Executor or Legal Representative

*Example*: Your will names a solicitor who also manages your estate. You provide them with a sealed envelope containing recovery instructions and account summaries, or similar in a digital formal (e.g. password-protected encrypted document).

Pros:

* Experienced with formal asset management and legal procedures.
* Neutral third party reduces the chance of family disputes.
* Likely to maintain better records and follow compliance protocols.

Cons:

* Costly; professional services usually involve fees.
* May lack understanding of specific digital platforms or systems.
* Less personal knowledge of your intentions or values.

### 5.1.3 Digital Steward or Technology-Literate Designee

(e.g., a friend, family member, or professional with IT knowledge)

*Example*: Your tech-savvy nephew is given access to your password manager's emergency contact feature, with prior walkthroughs on where to find key recovery codes.

Pros:

* Comfortable navigating digital platforms, security settings, recovery processes.
* Less likely to make technical errors that could result in data loss.
* May be more proactive in keeping backups and updating credentials.

Cons:

* Might lack legal authority if not formally designated.
* Could still face access issues due to password, encryption, or platform restrictions.
* Responsibility may be burdensome without adequate instructions.

### 5.1.4 A Team Approach

(e.g., one person for legal/financial oversight, another with technical abilities)

*Example*: Your sister handles your financial accounts and legal affairs, while your longtime friend—an IT admin—receives your digital access instructions and oversees social media and cloud accounts.

Pros:

* Combines strengths—technical expertise and legal/fiduciary competence.
* Distributes workload to avoid overwhelming one individual.
* Reduces the risk of single points of failure.

Cons:

* Requires clear coordination and well-defined roles.
* Potential for miscommunication or conflicting actions.
* More complex to set up legally and practically.

## 5.2 Communicating Your Wishes (miki b)

Clearly conveying your intentions helps your designee act confidently and reduces the chance of missteps. Below are options for how to communicate your wishes, with associated pros and cons.

### 5.2.1 Written Instructions (Printed Document)

Pros:

* Easy to update and share.
* Simple to create with minimal tools.
* Familiar and accessible to most people.

Cons:

* Must be securely stored to prevent unauthorized access.
* Can be lost, damaged, or outdated.
* Physical copies may not scale well for complex instructions (e.g., for many accounts).

### 5.2.2 Password Manager with Emergency Access Features

(e.g., LastPass, Bitwarden, 1Password)

Pros:

* Centralizes all credentials and sensitive information.
* Some allow emergency access by a trusted contact.
* Easy to revoke or update access.

Cons:

* Requires your designee to understand how to use it.
* Dependent on a third-party service that may change policies or cease operations.
* Requires initial setup and ongoing maintenance.

### 5.2.3 Encrypted Digital File with Instructions and Credentials

Pros:

* Can be stored securely on local devices or in cloud storage.
* Encryption adds security against unauthorized access.
* Scalable and customizable.

Cons:

* Requires technical understanding to decrypt and access.
* File could be corrupted or become inaccessible over time.
* Decryption key must be securely communicated separately.

### 5.2.4 QR Codes or NFC Tags to Key Resources

(e.g., QR code on a card linking to a secure vault or recovery file)

Pros:

* Easy for your designee to scan and access.
* Can be discreetly placed or distributed.
* Useful for quick recovery steps or pointing to more detailed info.

Cons:

* Still dependent on the security and reliability of the target storage.
* Could be scanned by unauthorized persons if not well protected.
* Requires setup and ongoing management.

### 5.2.5 Verbal Communication with Follow-Up Written Summary

Pros:

* Allows for detailed personal explanation and answering of questions.
* Builds trust and clarity.

Cons:

* Memory is unreliable; details can be forgotten or misunderstood.
* No formal record unless also documented.
* Not appropriate for complex or multi-step instructions.
* *Death doulas, palliative care workers, hospital staff, legal advisors - can help with knowledge and working out how to communicate*
* *When? How to keep info safe? How to avoid misuse? Consider elderly abuse*
* *Printed docs - kept by lawyers as addendum to wills? Website - QR codes? Need security of information.*
* *Lists, checklists,*
* *Look out for different laws around what is mentioned in wills. May not be enough to allow access*
* [*https://www.afcc.com.au/wp-content/uploads/2024.8\_AFCC\_Things-My-Family-and-Loved-Ones-Should-Know\_FA\_Fillable.pdf*](https://www.afcc.com.au/wp-content/uploads/2024.8_AFCC_Things-My-Family-and-Loved-Ones-Should-Know_FA_Fillable.pdf)

## 5.3 Accessing Credentials

*> Author Hint: Suggest documenting how your estate manager gets passwords, passkeys, OTPs, etc.*

## 5.4 Secure Storage and Timing

*> Author Hint: Explain how to prevent premature access. Consider locked safes or delayed release systems.*

## 5.4 Notifying the manager after the individual’s passing

*> Author Hint: How do you notify the manager? What does the manager have to do to start working through the individual’s estate? Write with recognition that the mechanisms are likely different around the world. Generalized list, followed by a US-based example may be useful. If we have any info on other countries, include them here or in an appendix. Miki mentions data for Japan, there may be others.*

## 5.5 Executing the plan

<Document a list of obligations for executors of a digital estate: first 30 days, first 90 days, etc.. Keep the focus on two audiences: 1) Pro-active person creating the estate plan; 2) Reactive person executing the estate plan

\* Useful prioritization for each actor, may need to reorg this into different sections

\* https://github.com/openid/death-and-the-digital-estate/issues/37>

# 6. Legal Considerations

## 6.1 Sharing With an Estate Attorney

## 6.2 Compliance and Storage Considerations

# 7. Managing a Digital Estate Reactively

While the majority of this document discusses how one should plan the handling of their digital estate, there is a reality, which this section addresses, one in which an individual has passed and not planned or stated their wishes and it now falls to you to address.

If you find yourself in such a situation, your focus should be on gaining critical points of control over the individual’s digital estate. You should, in this moment, be attempting to retroactively cover all of the topics this document has discussed above, but instead focus on the few very important accounts and services that, over time, will help you manage the individual’s larger digital estate. The goal is not to use the individual’s estate or to impersonate them, but to gain access and control when or if you need to use them.

The following is not an exhaustive list of things to be done but instead a list of suggestions to focus upon in the near term to enable you to, at your own pace, deal with other digital identity related issues with fewer concerns for loss, misuse, and fraud.

That being said, please proceed cautiously. Haley Perry in her [New York Times article](https://www.nytimes.com/wirecutter/reviews/advice-password-recovery-after-death/) dated 25 June 2025 wrote:

Even if you do have the password, note that logging in to someone else’s computer or online account [is illegal](https://hacked.com/hacking-and-its-legal-consequences/) under the [Computer Fraud and Abuse Act](https://www.justice.gov/jm/jm-9-48000-computer-fraud), and we advise treading lightly and refraining from acting as the account owner. If you are the inheritor of the estate, you still need to [abide by the terms of service](https://www.rochelegal.co.uk/do-your-family-have-the-right-to-access-your-online-accounts-after-your-death/) for each account to see if the contents are legally transferable. We suggest speaking to a lawyer who can better help you understand the privacy laws for the accounts you want access to.

Again your goals should be to gain access and control, not to start using the individual’s digital estate as if it were yours. Things not to do immediately (or potentially ever):

* Start resetting the individual’s passwords
* Using the individual's digital services on their behalf

Lastly before discussing what should be done, this section of the document is written with the assumption that you are the person the individual has previously identified as the one to handle their estate, both physical and digital. But it is also likely that you might be someone that the executor of the individual’s estate or a close survivor has asked to assist them. If that is the case, make all efforts to document what steps you are taking and ensure that the executor is aware of your actions.

With respect to the individual’s digital estate consider the following areas to focus upon:

* **Mobile Phone and Email**: Identify and hopefully determine whether you can access the individual’s mobile phone and/or email
  + This will, in the future, enable you to receive one-time passwords delivered by SMS or email. The thought being that the individual, for the most services, had registered for these additional authentication factors.
  + Consider transferring the phone number or at least billing to yourself. This will prevent the phone line from being terminated due to non-payment. Telephone carriers have a process for such a transfer.
* **Password manager**: Ideally the individual had some form of password management system. Depending on the degree of tech savviness such a system might be a notebook of handwritten usernames and passwords or a printed list of the same. It might be an operating system or browser-based password manager (e.g. Apple Passwords, Google Password Manager, Samsung Pass, etc) or a third party password management service (e.g. 1Password, LastPass, etc.)
* **Laptop, tablet, and/or mobile phone:** The previous items strongly imply that you will need to learn where the individual’s physical devices are. Ensure that you not only inventory and identify the devices but also ensure that you locate the necessary charging cables and plugs.
* **Legal and financial identity:** Sadly fraudsters have no respect for those who have passed. To prevent the individual’s legal and financial identity from being used in a fraudulent manner, you will need to contact the credit bureaus to alert them to the passing of the individual. This can help stop future fraud from happening.

Appendix:

# Glossary of Terms

# Actions in the first 90 days post-death - by country

## {{Country}}

### Days 0-7

### Within 30 days

### Within 60 days

### Within 90 days

## 

## Ireland

### Days 0-7

* Get medical certificate of cause of death from doctor or hospital,
* register death with local civil registration office,
* bring medical certificate,
* PPS number of deceased.
* You will receive a Death Certificate which is essential for other tasks.
* Arrange the funeral.

### Within 30 days

* Notify the Department of Social Protection to stop pension or apply for survivor benefits;
* Tax Office to update tax records and cease liabilities;
* local authority if the deceased rented social housing or had property tax obligations.
* Secure deceased’s property,
* cancel or redirect mail,,
* cancel or transfer utilities,
* notify banks to freeze accounts.

### Within 60 days

Locate the Will and find out who is the executor. If no will apply for a grant of probate to administer the estate. This can take months. Apply for relevant social welfare payments, e.g. widow’s pension. Notify insurance companies, credit card companies, credit bureaus, employers or pension funds. Assess the estate assets and debts, engage a lawyer (solicitor) if needed. Pay outstanding bills, debts and cancel subscriptions.

## UK

### Days 0-7

Similar to Ireland except a death certificate is needed to get a certificate allowing go ahead for burial or cremation (this can take up to 2 weeks).

### Within 30 days

Notify Government departments via the “Tell Us Once” service. Automatically alerts tax, DWP, drivers license, vehicle ownership, passport office, local council.

## USA

### Days 0-7

obtain legal pronouncement of death. Hospital or nursing home staff will do this. At home, call 911 to have a doctor confirm. Contact a funeral home or cremation provider. They will help file for the death certificate and provide guidance.

### Within 30 days

get 10-15 certified copies of the death certificate via the funeral home or local vital records office. Find the will and identify the executor. If there is no will, the court will appoint an administrator under intestate laws. Notify SSA, employer, banks, mortgage, credit cards, insurance companies, utilities. Cancel or transfer key services: drivers license, social media and email accounts, subscription, memberships, online services, voter registration.

### Within 60 days

open probate or file a small estate affidavit if no will. Open an estate bank account for depositing incoming funds and paying estate bills. Start making an inventory of assets and debts.

### Within 90 days

File for any available benefits, including life insurance claims. Notify the IRS (form 56). Later you will file an income tax return. Assess the need for legal / financial advisors.