



CREATE A DIGITAL ESTATE PLAN

By Larry Richman

Updated July 24, 2025

In this increasingly digital age, much of our social and financial information lives in the cloud. Photos, social media accounts, financial accounts, Church records, and other digital files all have value. Since this digital information will outlive us, it is important to determine how you want that information handled after you die. You can either make arrangements now or leave it to your family and estate executors to sift through your virtual remains.

Do you want the records you have created on FamilySearch to be accessible to your family? What about your personal annotations in the Gospel Library app? What about your photos and videos on the cloud? An executor won't automatically have access to an online account unless you make previous arrangements.

In a digital estate plan, you can give instructions to your heirs about what to do with all these assets. For your social media accounts, should they leave the accounts active or download photos to share with family and then delete the accounts?

A digital estate plan should be part of a comprehensive estate plan, which should include a Last Will and Testament, a Power of Attorney. It may also include a family trust.

MAKE A PLAN FOR YOUR DIGITAL ASSETS

For each of your accounts, you will need to determine which should be canceled and which you want to transfer to your heirs. For example, if you have a Google Photos account, determine if you want someone to download your photos and share with others, transfer the account to a family member to maintain it, or if you simply want it deleted.

For online accounts that have automatically renewing charges, do you want someone to cancel them, or do you want a family member to maintain them?

MAKE AN INVENTORY

Make a list of your digital assets, such as those listed below.

- **Social media accounts** (such as Facebook, Twitter, Instagram, LinkedIn, Pinterest, YouTube, and blogging sites). These accounts may have important photos and videos, as well as important historical information in posts.
- **Photo- and video-sharing accounts** (such as Flickr, Photobucket, Picasa, and Google Photos). Indicate what should be done with your photos and videos. Do you want them shared with your extended family, with friends, or with coworkers? Are there certain photos and videos that you want deleted?
- **Email accounts.** Note that access to email accounts can be critical. They may contain important information about other digital assets. You may also need access to the email accounts to reset passwords and gain access to other accounts.
- **Online storage accounts** (such as Box, Dropbox, Google Drive, and iCloud) and computer back-up services (such as [Carbonite](#)) may contain important files.
- **Financial accounts** (such as bank accounts, brokerage accounts, credit card accounts, online bill-payment accounts, cryptocurrency accounts, PayPal, Venmo, and Cash app) may have monetary balances.
- **Benefit accounts** (such as airline frequent flier accounts, loyalty cards, car rentals, and hotels) may have valuable balances.
- **Online gift cards** with balances.
- **Shopping sites** and store accounts (such as Amazon, Costco, Walmart, Target, Etsy, and eBay). Some may have outstanding orders, credit balances, digital gift cards, or rewards points.
- **Church accounts** (such as FamilySearch, notes and annotations in the Gospel Library app, goals, impressions, and annotations in the Gospel Living app).
- **Subscriptions to services** (such as video streaming services, subscription websites, and online newspapers and magazines).
- **Utilities** and other services that have automatic payments (such as phone, electricity, water, gas, garbage, internet, cable television, gym memberships, and insurance policies).
- **Voicemail accounts** that may have important messages.
- **Video gaming accounts** with in-app purchases and in-game assets.
- **Business assets** (such as client accounts payable, copyrighted materials, trademarks, software code, domain names, or other intellectual property that generates revenue).
- **Computers, tablets, and smartphones.** Provide passwords or PINs to log in to each device.
- **Wi-Fi.** Provide passwords for your home or office Wi-Fi.

For each asset, indicate who you want to take care of it and provide instructions on how to access the account and what should be done with it. Include the username, account number, password, email address and phone number associated with the account, PIN codes, and answers to secret questions. For sites that require two-factor authentication, be sure that your representative will have access to the cell phone or email address that is designated to receive

the authentication codes. Be sure to include passwords and PINs for phones and computers where files are stored. If files are encrypted, provide passwords for the files.

Consider using an inventory tool and a password management system to keep track of these records. [LastPass](#) is a password manager that organizes and protects your passwords. It can automatically log you into websites, but it is also a great tool to maintain an encrypted list of accounts, usernames, passwords, and other information about sites. One master password unlocks the data, so it is easy to retrieve and update the information.

Keep the inventory list safe. Do not save the list on your computer or back it up in the cloud. I recommend you keep it on a USB drive that you store in a fire safe in your home with a duplicate copy in a safety deposit box in a bank. Keep it relatively accessible since you will need to periodically update it as you set up new accounts or change passwords. No matter how trusted your designated representative, you probably do not want to provide her or him access to your accounts prematurely. But you can leave instructions so that after your death, the USB drive and/or the master password to LastPass can be given to your designated representative.

GAIN ACCESS TO ACCOUNTS

The legal way to access your accounts after you die depends on the laws of the country and state where you live, the type of account involved, and the terms of service of the company involved. Many states in the United States have adopted the Revised Uniform Fiduciary Access to Digital Assets Act, which guarantees individuals the right to transfer digital possessions to a legal representative after their death. You can grant power to that legal representative through a will, power of attorney, or trust. Work with an estate planner or lawyer to make sure you prepare the proper documents and that your designations comply with your state's laws.

Appoint a digital representative who will handle the disposition of your digital assets, working with the general executor of your estate according to your instructions in your Last Will and Testament.

Some companies require your legal representative to follow a specific process to gain permission to your accounts, including providing them a copy of your death certificate. Although it would be easier for your heirs to just log into your accounts, some sites may not permit sharing passwords, and they may consider your representative in breach of their terms of service.

In some cases, a company may cancel your account and delete the data if an unauthorized user gains access. Some companies do not allow any access after a user is deceased. Others delete or freeze accounts when they learn that the user has died. Review the terms of service for each company. In some cases, the terms of service can be overridden by a court order.

Some companies make it easy by giving you a way to indicate whether someone else should have access to your account after you die. With Facebook, for example, you can decide in advance if you want Facebook to delete your account upon your death or you can name someone to manage portions of your account after you die. That way, your representative

could post a tribute with information about your funeral or update your profile photo and cover picture. See the account-specific information in the next section of this article for instructions for various companies who provide options for advanced directives.

ACCOUNT-SPECIFIC INFORMATION

This section provides instructions for some companies that provide options for advanced directives.

Ancestry®

Ancestry.com does not allow the transfer of ownership of an Ancestry® family tree, but you can share trees and copy trees and people between accounts. See the Ancestry® page [“Transferring Ownership of an Ancestry® Family Tree.”](#) Contact Ancestry® to see if a first degree relative can request to take over as site manager.

If you delete your account, all information on your account (including, but not limited to, family trees, records, photos, and DNA results) will be permanently deleted. You may cancel your subscription and the data will be retained. See the Ancestry® page [“Deleting Your Ancestry® Account.”](#)

Apple

You can name a Legacy Contact who can have access after your death to your photos, videos, notes, documents, and personal information after your death. To set up a Legacy Contact, go to Settings, tap Apple Account next to your name and photo, tap Sign-In & Security, then choose Legacy Contact.

Alternatively, a deceased person’s legal representative must obtain a court order that names the person as the rightful inheritor of the deceased. Read more details on Apple’s page [“How to request access to a deceased family member’s Apple accounts.”](#)

Music and video files in the account are not owned by the account holder but are licensed for the original account holder’s lifetime. Therefore, there is no right of survivorship.

Apple devices, such as iPhones and iPads, that are locked with a passcode are protected by passcode encryption, and unless the next of kin knows the device passcode, Apple will not be able to remove the passcode lock on the device. You can perform a factory reset so the device can be reused, but all the data from the device will be deleted.

Church of Jesus Christ of Latter-day Saints

You can create digital information in various Church systems, such as Gospel Library and Gospel Living. Over a lifetime, you may build a treasure of study notes, including personal insights and inspiration. You may want this information to stay private or you may want to pass these

records to your posterity after you die. The Church makes it easy for you to indicate your preference.

What Happens When You Die

When you pass away, your Church Account is locked to protect your privacy and personal information. But the information you have created, such as notes and highlights on the Gospel Library mobile app and ChurchofJesusChrist.org are not immediately deleted.

What You Can Do Now

While you are living, you may designate your family and descendants as legacy contacts which gives them access to your content after your death. If you do not make a choice while living, and a family member or legal representative has not contacted the Church within two years, then your data may be deleted.

To indicate your preference, go to account.ChurchofJesusChrist.org/legacyContacts and indicate one of the following choices: (1) do not share my Gospel Library data with others after my death or (2) allow my family and descendants to access my notes and highlights after my death.

A spouse, parent, or legal custodian of the estate can request access to a deceased relative's notes and annotations. The frequently asked questions page shows how to access notes created by a deceased family member.

Computers and Other Devices

Computers, laptops, and smartphones have policies that vary between brands. If you want your family to have access or control over your physical devices after you die, you should provide them the passwords now. Even if the company has the means of granting access to devices, most companies are not willing to do so. Most devices provide the ability to perform a factory reset so the device can be reused, but all the data from the device will be deleted.

Dropbox

If Dropbox is syncing to your computer, all your Dropbox files will be on your computer. Therefore, if your heirs have access to your computer, they can access your files. But if it is not syncing to your computer, your heirs would need your login credentials to access the files.

Dropbox determines inactive accounts by looking at sign-ins, file shares, and file activity over the previous 12 months. Once an account is determined inactive, Dropbox deletes the files on the account. To request access to the account of a deceased person, a legal representative must send the appropriate documents by physical mail. See Dropbox's page "[How to access the Dropbox account of someone who has passed away.](#)"

Facebook

Facebook lets you decide in advance if you want your account to be deleted upon your death or you can name someone as a Legacy Contact with the right to manage portions of your account, which will be turned into a memorial page, essentially freezing the page in time. If you name a Legacy Contact, that person can do the following:

- Manage tribute posts on your profile, which includes deciding who can post and who can see posts, delete posts, and remove tags.
- Request the removal of your account.
- Respond to new friend requests.
- Update your profile picture and cover photo.

Your legacy contact can only manage posts made after you die. They will not be able to post as you or see your messages while you are living. You can also indicate whether you want your Legacy Contact to download a copy of what you have shared on Facebook. This will include posts, photos, videos, and information from the About section of your profile, which might be content that was not originally visible to your Legacy Contact. Messages will not be included.

If you don't want a Facebook account after you die, you can request to have your account permanently deleted instead of choosing a Legacy Contact.

For more information see “Memorialization Settings” in your Facebook account settings and the [Facebook help page about Legacy Contacts](#).

FamilySearch

See the section “Church of Jesus Christ of Latter-day Saints” above.

Google

Google will work with immediate family members and representatives to close the account of a deceased person where appropriate. In certain circumstances, they may provide content from a deceased user's account. In all these cases, Google's primary responsibility is to keep people's information secure, safe, and private. They do not provide passwords or other login details. Decisions to satisfy a request about a deceased user are made only after a careful review.

Google's Inactive Account Manager lets you plan what happens to your data if you stop using your account. (Access it in “Data & Personalization in your Google account.”) The Inactive Account Manager lets you decide in advance when Google should consider your Google Account inactive, choose who to notify and what to share, and decide if your inactive Google Account should be deleted. The plan you set up is only triggered after you haven't used your Google Account after several months of inactivity. (You can choose options of 3–18 months.)

Google lets you select up to 10 trusted contacts who can access your Gmail, photos, and more if your account is inactive for several months.

Learn more on the Google page “[About Inactive Account Manager](#).”

Gospel Library

See the section “Church of Jesus Christ of Latter-day Saints” above.

Gospel Living

See the section “Church of Jesus Christ of Latter-day Saints” above.

Hotmail

See the entry “Microsoft” below.

iCloud

See the entry “Apple” above.

Instagram

Instagram lets you memorialize the account of someone who is deceased. Memorialized accounts have the following key features:

- No one can log into a memorialized account.
- The word “Remembering” will be shown next to the person's name on their profile.
- Posts the deceased person shared, including photos and videos, stay on Instagram and are visible to the audience they were shared with.
- Memorialized accounts don't appear in certain places on Instagram, like Explore.

Once memorialized, no one will be able to make changes to any of the account's existing posts or information. This means no changes to the following:

- Photos or videos added by the person to their profile.
- Comments on posts shared by the person to their profile.
- Privacy settings of their profile.
- The current profile photo, followers, or people the person follows.

For more information see the [Instagram page about memorialized accounts](#).

iTunes

See the entry “Apple” above.

LinkedIn

LinkedIn has a process to remove the profile of a deceased person. A family member or others may submit a request using the [LinkedIn Profile Removal form](#) and providing a link to an obituary or relevant news article.

Live

See the entry “Microsoft” below.

Microsoft

For Microsoft accounts (including Hotmail, Live, MSN, or Outlook), next of kin do not need to contact Microsoft to let them know that someone has died or has become incapacitated. If a deceased person’s representative knows the account credentials, she or he can close the account his or herself. If the representative does not know the account credentials, it will be closed automatically after two years of inactivity. See the page “[How to close your Microsoft account.](#)”

If you don’t have the username and password to log in to Microsoft email accounts (Hotmail, Live, MSN, or Outlook), you can submit a [Next of Kin request](#) and Microsoft will send you a DVD with all the emails, attachments, address book, and contact lists from the email account.

See the Microsoft page “[Accessing Outlook.com, OneDrive and other Microsoft services when someone has died.](#)”

MSN

See the entry “Microsoft” above.

MyHeritage

Contact MyHeritage to see if a first-degree relative can request to take over as site manager.

If you delete your account, all information on your account (including, but not limited to, family sites, family trees, records, photos, and DNA results) will be permanently deleted. See the MyHeritage page “[How do I delete my account on MyHeritage?](#)”

OneDrive

See the entry “Microsoft” above.

Phones

See the entry “Computers and Other Devices” above.

Pinterest

Pinterest will deactivate the profile of a deceased person if requested by a family member. The site will not give out any personal or login information following the death of a user. See the Pinterest page [“Deactivate or close your account.”](#)

Outlook

See the entry “Microsoft” above.

Tablets

See the entry “Computers and Other Devices” above.

Twitter

In the event of the death of a Twitter user, an immediate family member or a person authorized to act on behalf of the estate may contact Twitter to download the person’s tweets and have an account deactivated. Previously published tweets are not removed, and no further tweets may be posted.

Wikipedia

Users who have made at least several hundred edits or are otherwise known for substantial contributions to Wikipedia can be noted at a central memorial page. Wikipedia user pages are ordinarily fully edit-protected after the user has died, to prevent vandalism. See the Wikipedia page [“Deceased Wikipedians/Guidelines.”](#)

Yahoo!

Yahoo allows a legal representative to request that a deceased person’s account be closed, and any contents deleted. Yahoo cannot provide passwords or allow access to the deceased's account, including content such as email. See the Yahoo page [Options available if a Yahoo Account owner passes away.](#)

YouTube

See the entry “Google” above.

Zoom

See the article [“Changing the account owner.”](#)

The information provided here is for educational purposes only and does not constitute legal advice or an endorsement of any third party. Any hyperlinks to third-party content are intended to provide additional perspective and should not be construed as an endorsement of any services, products, or points of view. Some links are affiliate links to products and services for which we may receive compensation for referring customers.

This is not an official publication of [The Church of Jesus Christ of Latter-day Saints](#). The views expressed herein are the opinions of the author and do not necessarily reflect the views of the Church. The Church of Jesus Christ of Latter-day Saints and FamilySearch are trademarks and service marks of The Church of Jesus Christ of Latter-day Saints or Intellectual Reserve, Inc., and may be registered in the United States and other countries.