Password Managers

# Password Managers

* [**Using LastPass Enterprise**](using-lastpass.html)

## Overview

[Ministry of Justice (MoJ) guidance](passwords.html) makes clear that you should have different passwords for different services. These passwords must be complex.

But how do you remember all these different passwords?

The simplest way is to use a [Password Manager](https://en.wikipedia.org/wiki/Password_manager). If you have lots of different, and complex, passwords for all your accounts, using a password manager makes life much easier.

This article provides guidance on using password managers within the MoJ.

## What is a password manager/vault?

A password manager stores sensitive information in an encrypted form. Password managers are sometimes called password vaults.

In the MoJ, 'password managers' are tools that you might use for your personal accounts. 'Password vaults' are tools that a team of people might use to look after details for shared accounts.

Password vaults usually have extra strong access controls, such as hardware tokens.

Here, we use 'password manager' and 'password vault' interchangeably, except when stated otherwise.

### When do you use a password manager or a password vault?

The following table shows when you might use a password manager or vault:

|  |  |  |
| --- | --- | --- |
| Scenario | Tool | Notes |
| Single user, personal accounts | Password manager | For accounts that only you use, or have access to, then you would probably store the details in a password manager. An example would be storing the username and password for your work email account; only you should have access. |
| Multiple users, shared accounts | Password manager or password vault | Some accounts might be shared between a group of users. For example, a team might need to know the password for an encrypted document. If the access required is for a sensitive or operational system, then a more heavily protected tool such as a password vault might be appropriate. |
| System access, no human use | Password vault | Some MoJ systems need to 'talk' directly to other systems. No humans are involved in the conversation. The passwords protecting these communications can - and should - be extremely complex. A strongly secured password vault would be ideal for this purpose. |

## Best practices

The NCSC is [very clear](https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers):

"Should I use a password manager? Yes. Password managers are a good thing."

This is helpful for us in the MoJ, as much of our IT Policy and guidance derives from NCSC best practices.

## What makes a good password manager?

A password manager should never store passwords in an unencrypted form. This means that keeping a list of passwords in a simple text file using Notepad would be A Bad Thing.

Good password managers encrypt the passwords in a file using strong encryption. It shouldn't matter where you store the encrypted file. Storing the list 'in the cloud' lets your password manager access the data from any device. This is useful if you are logging in from a laptop, or a mobile device. Storing the passwords locally means the password manager works even when offline.

A good password manager will have:

* Strong encryption for the list of passwords.
* Network access for encrypted lists stored 'in the cloud'.
* A dedicated app but also a 'pure' web browser method for working with your password list.
* A tool to generate passwords of varying complexity.
* The ability to fill in login pages.

## What password manager should I use?

In the [NCSC article](https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers), they are very careful not to identify or recommend a password manager. This ... caution ... is the reason why we don't say much about password managers within the MoJ guidance.

There are several password managers used within the MoJ. [LastPass](https://www.lastpass.com/) and [1Password](https://1password.com/) are probably the most popular for personal or team passwords. Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at LastPass and 1Password. See which one you like best, and try it out. When you decide on a password manager, request approval from your line manager to install and use it: "I'm planning to install and use XYZ to manage my passwords, is that OK?".

See also [Using LastPass Enterprise](using-lastpass.html).