# Using cloud services – considerations for individuals

information commissioner
Barrantagh Fysseree

**What is cloud storage?**
There are an increasing number of services offering 'cloud storage' where you can upload documents, photos, videos and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet etc).

**How do they work?**
Once you have registered for an account you typically create a folder on your computer and every file you place in that folder is copied to the servers of the storage provider. Any changes made to these files are automatically copied across and immediately accessible from other devices you may have.

Most provide a limited service for free with paid-for versions allowing greater or even unlimited storage space.

**What does this mean for my personal information?**
If you choose to store your files in the cloud you need to remember that this means they are really just stored on servers controlled by the service provider. Some providers of cloud services may also use the cloud services of another organisation.

This means you need to check that the security and availability of the service is right for the types of files you want to upload.

**Using cloud storage to share files**
Using cloud storage services means that you and others can access and share files across a range of devices and locations.

Files such as photos and videos can sometimes be difficult to email if they are too large or you have a lot of them. Uploading to a cloud storage provider means you can quickly circulate a URL and you can share your files with anyone you choose.

**Using cloud storage to store files**
You might also use cloud storage services to keep copies of important files outside your home as part of a backup solution. This means that in the event of a disaster in your home (eg fire, flood or theft) you still have copies of your data.

**What should I think about when placing personal information in the cloud?**

1. Think carefully about who can access your files

Cloud storage services typically allow you to set one of three settings to control who can view your files:

- private – only you can view the files (although the cloud storage provider may still be able to view your files);
- public – everyone can view the files without any restriction; or
- shared – only people you invite can view the files

These settings might be applied to individual files or to all files within a specific folder.

2. Choose your passwords carefully

Like most online services, access to your files will be controlled by your username and password. It is good practice to use a unique and strong password for each online service, especially if you are storing important files in the cloud. If you use the same username and password across many different sites and one of these sites is hacked, the attackers might attempt to use those credentials to access your other online services.

3. Check the storage provider's terms and conditions and privacy notice

A good cloud storage provider should have clear and transparent information on their website about how they will secure your personal information and what they will or will not do with it. If you cannot find this information or feel terms are unfair or unclear, shop around and compare the information.

4. What type of encryption does your cloud storage provider offer?

A cloud storage provider might store your data in an encrypted form and keep the key in a safe and secure location. When you use your username and password to log into the service they will decrypt your files so that you can access them. This means that you can invite other people to log in and view your files because the storage provider manages the encryption.

Data can be encrypted by your web browser so that whilst it is being sent between you and the cloud storage provider it cannot be read or modified along the way. If you are using a web browser you will see a padlock symbol and the URL will start with 'https://'. Once your files are received by the cloud provider they will be decrypted so if you want your files stored in an encrypted form you should encrypt them before you send them or use a cloud storage provider who encrypts them on your behalf.

5. Can you encrypt your information before placing it in the cloud?

The most secure way to use a cloud storage service is to encrypt your files before they leave your computer. If you hold the encryption key, no one else will be able to easily decrypt your files and therefore read or use your personal information. Whilst this is a good approach for a storage or archive service it will not be possible to share these files with anyone without also sharing the encryption key which can be difficult to manage.

If this is important for you, you can look for a cloud storage provider which has included this as part of their product or you can do it yourself using software from a trusted and reliable third party. There are also a number of free or low cost encryption software tools available but remember that when obtaining software from the internet you should make sure this comes from a reputable source and you check reviews to ensure that the software has been tested against the claims that it makes.

It is important to remember that if you lose or forget the key you will not be able to decrypt your files.