# Backups

## Keep your data safe

**Over 88% of UK households own a computer, meaning that most of us regularly access, use and store personal digital material.**

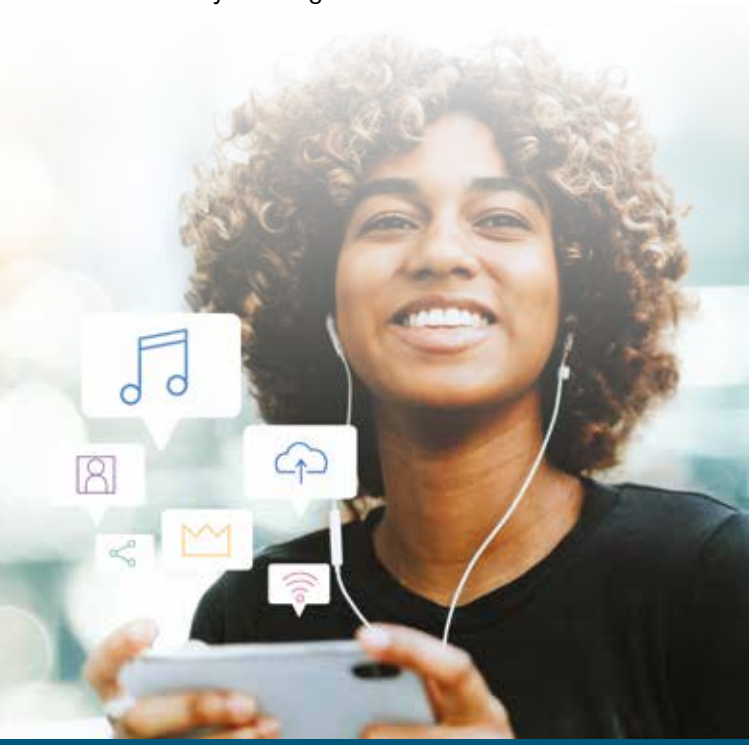
**This could be sensitive financial information, a music collection, documentation, or precious pictures of family.**

**Simple steps can be taken to help ensure this data is protected from damage, cyber attacks or online fraud.**

## What is a backup?

A backup is a copy of computer data taken and stored elsewhere so that it can be used to restore the original after a data loss event.

It's like taking out insurance on your possessions, your house or your car. It means that should your data be lost, stolen, or damaged, there is a strong chance that you can get it back.



## When should I backup my data?

Your data is only as safe as your last backup, so the best advice is to backup at regular intervals.

Businesses should consider backing up data every week with daily backups for important data. If you are a personal user, you may make limited changes to your content and need to do this less often. It is important to work through your requirements and make a plan to keep your information safe.

## What do I need to back up?

Everyone's data is different, so what to backup will depend on what you store and how you use it.

It's important to review your systems and data regularly, so that you can identify what is needed for a disaster recovery plan and backup accordingly.

As a business, you might want to backup entire systems to ensure you can get back up and running as soon as possible in the event of an incident. As a personal user, you may only wish to backup precious documents or files.

When making this decision – ask yourself the question – 'could I manage without this data?' If the answer is 'no' then it would be wise to back it up.

## How can I backup my data?

Before you start, a review of your systems and the amount and type of data you use will help identify how you should backup safely. Backup options vary in terms of price, space, speed, and security levels.

The security of your data could be affected by many things – a computer malfunction, a fire, a flood, a hacker or a burglar. Consider all these possibilities and choose the backup option that best suits your needs.

**USB stick / external hard drive**

Infrequent users with small amounts of data may be able to use a USB stick or an external hard drive, which can be purchased at a low cost. They are simply plugged into your device and files can be copied over. Always ensure the backup device is removed after use.

### Cloud storage

Cloud storage enables your data to be stored on another company's infrastructure which almost guarantees it is separate from your network and systems. Many cloud backup solutions come with protection from viruses, malware and ransomware, meaning that your data is almost always going to be protected.

Personal users of Microsoft and Google may already use cloud services for storage of e-mail and documents – especially if they use OneDrive or Google Drive. Both of these services offer automatic synchronisation with the cloud. Other services such as Dropbox are also available and can easily be set up.

### Encryption

Some backup methods will encrypt your data, adding an extra level of security to protect your information. Businesses with large amounts of sensitive or personal information may choose a provider that can ensure this advanced level of security.

Any access to backups should be restricted and any device used for a backup should never be left connected (either physically or over a network).

*'could I manage without this data?' If the answer is 'no' then it would be wise to back it up.*

## What else do I need to know?

Once you have reviewed your data and chosen how best to backup your information, it's a good idea to test your backup and restore process.

It's important to know how the process works – how to access your backups, how to decrypt your information if necessary, and how to restore it.

To replicate a real disaster, try doing this with a brand-new machine so you know you can get 'back up' and running in the shortest possible time.

Remember, backups are important ways of protecting personal data. They should be used alongside other security methods to protect against viruses and ransomware as part of an overall data security plan.

If you want to know more about data protection as an individual or a business, you can access advice and information on a range of cyber security topics at the following sites:

**www.ncsc.gov.uk**

**www.cyberaware.gov.uk**

**www.takefive-stopfraud.org.uk**

**www.actionfraud.police.uk**

**www.serocu.police.uk/individuals**

Report online at **www.sussex.police.uk** or **www.surrey.police.uk** or **call 101**.
In an emergency always **call 999**.

Find us on social media

Produced by Sussex Police Corporate Communications 2019