Department for Levelling Up,
Housing & Communities

Overview of backup best practice

V1.3

LOCAL DIGITAL Cyber

What is a backup?

- A backup is a copy of your important data that's stored in a separate safe location, usually in the Cloud or on removable media
- Once you've made a backup, if you lose access to your original data, you can restore a copy of it from the backup
- Most backup solutions allow you to choose what data is backed up, whether that's just documents or the entire contents of your server/computer
- You should back up anything that you value. That is, anything that would inconvenience you if you could no longer access it

LOCAL DIGITAL Cyber

Why might I need a backup?

There are many reasons why you might need a backup.

- You have a new device, and you want to copy existing files onto it
- Your device is lost, stolen or broken
- The data on your device is accidentally deleted
- A virus (or other type of malware such as ransomware) may erase your data, or prevent you from accessing it
- Your hard drive needs to be erased or replaced

LOCAL DIGITAL Cyber

How often should a backup take place?

- Many factors affect the frequency of backups, including:
    - The amount of data
    - The sensitivity of the data
    - How often it changes
    - How quickly you want it restored
- For example, if some data only changes once a month, backing up the data every day is probably excessive. Similarly, if the data changes every hour, then a daily backup is not enough

LOCAL DIGITAL Cyber

Backup retention period

- Backups must be stored and kept available to restore the data when required. The length of time that backups are kept for recovery purposes is called the ‘retention period’

- When backup data is no longer required for recovery purposes, it is deleted, to comply with data protection requirements. Sometimes, the data must be retained for a longer time

- Backup data that is held for longer than the retention period is considered archive data, and is managed using the archive schedules. It is not normally used for recovery purposes

LOCAL DIGITAL Cyber

Backing up using Cloud storage

- Using Cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location
- You'll also benefit from a high level of availability
- Service providers can supply you with data storage and web services without the need to invest in hardware up front
- Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to the Council

LOCAL DIGITAL Cyber

Backing up using removable media

- Backing up using removable media allows you to backup large amounts of data, which may be beyond the capacity of Cloud storage options
- Setting a calendar appointment or reminder to do the backup at regular intervals is advisable if not using schedule automatic backups
- If you're given the option to protect your backup with encryption, you should do this. Personal or sensitive data should always be backed up
- When the removable media isn't in use, it's important that you disconnect it. Malware can move to attached media automatically, which means any such backup could also be infected

LOCAL DIGITAL Cyber

Keep your backup separate from your computer

- Whether it's on a USB stick, on a separate drive or a separate computer, access to data backups should be restricted so that they:
  - are not accessible by all staff
  - are not permanently connected (either physically or over a local network) to the device holding the original copy

- Malware can move to attached storage automatically, and infect any attached backup, leaving you with no backup to recover from

- You should consider storing your backups in the Cloud or a different location, so fire or theft won't result in you losing both copies

LOCAL DIGITAL Cyber

Restoring backups

- Once you've made your backup, it's important to check that they contain all your important data. For example, you might want to check that your Cloud storage contains new files or folders you have recently created

- If you have data that is 'irreplaceable', then consider keeping a copy in the Cloud and also on removable media, so you can always access it

- It is essential that regular restore testing takes place, to guarantee that system backup processes are working correctly and backed up data can be recovered

LOCAL DIGITAL Cyber

Staying in touch

Follow our progress

- Read our fortnightly sprint notes on Medium
- Follow LDCU on Twitter (@LDgovUK)
- Subscribe to our Cyber newsletter for progress updates and news relevant to those working in and around local government cyber security
- We'll also be sharing regular updates on the DLUHC Digital blog

Have your say

We welcome further collaboration and input, so if you would like to share with us any strong evidence to support our research please email cybersupport@localdigital.gov.uk.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

We welcome feedback on our cyber support service

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

LOCAL DIGITAL Cyber