Data and Analysis Storage

K-2.DA.7 Store, copy, search, retrieve, modify, and delete information using a computing device, and define the information stored as data.

3-5.DA.7 Explain that the amount of space required to store data differs based on the type of data and/or level of detail.

What is the best way to storage data?

The ideal approach to save data for a longer time is **cloud storage**. Data security and storage reliability are two advantages of cloud storage that can't be matched. In addition, end-to-end encryption ensures the safety of all transmitted data. **Cloud storage** is indeed the best way to store data for a longer period of time. By opting for cloud storage, the user will get high-quality data security as well as reliable data storage. Data protection is ensured with the employment of end-to-end encryption

Four Types of Computer Data Storage.

- Computer Data Storage #1: Cloud Storage.
- Computer Data Storage #2: Cloud Backup.
- Computer Data Storage #3: USB Flash Drive.
- Computer Data Storage #4: Optical Media Storage.

External storage devices

- External HDDs and SSDs. ...
- Flash memory devices. ...
- Optical Storage Devices. ...
- Floppy Disks. ...
- Primary Storage: Random Access Memory (RAM) ...
- Secondary Storage: Hard Disk Drives (HDD) & Solid-State Drives (SSD) ...
- Hard Disk Drives (HDD) ...
- Solid-State Drives (SSD)

Store Data Securely

Here are some practical steps you can take today to tighten up your data security.

1. Back up your data. ...
2. Use strong passwords. ...
3. Take care when working remotely. ...
4. Be wary of suspicious emails. ...
5. Install anti-virus and malware protection. ...
6. Don't leave paperwork or laptops unattended. ...
7. Make sure your Wi-Fi is secure.

1. Back up your Data

Create a back-up copy of your data, and do this regularly. Store it somewhere other than your main workplace, if possible. That way, if there's a break-in, fire or flood, you don't lose everything.

2. Use strong passwords

Make sure you, your staff, volunteers, and anyone else involved in your operations uses strong passwords - including smartphones, laptops, tablets, email accounts and computers.

3. Take care when working remotely

Make sure the devices you use are as secure as the equipment you use in the office. Also be mindful of your surroundings. If you're on a train, for example, it's relatively easy for other people to see your screen.

4. Be wary of suspicious emails

Educate yourself and those working for you on how to spot suspicious emails. Checking for obvious signs such as bad grammar, requests for you to act urgently, and requests for payment will help you avoid being caught out. If it looks suspicious, don't trust it – and warn your staff not to either.

5. Install anti-virus and malware protection

And keep it up-to-date. The National Cyber Security Centre has some useful advice and guidance on cyber security.

6. Don't leave paperwork or laptops unattended

Data breaches can occur when staff and volunteers leave paperwork or laptops unattended. This could be in the boot of a car, on a train, or at home. Make sure you take steps to protect the personal data you hold by being vigilant and storing it securely away when it's not in use.

7. Make sure your Wi-Fi is secure

Using public Wi-Fi or an insecure connection could put personal data at risk, so you should make sure you always use a secure connection when connecting to the internet.

8. Lock your screen when you're away from your desk

And make sure your staff do the same. Taking steps to lock your screen when you leave your desk is a simple thing to do, but will prevent someone else from accessing your computer.

9. Keep on top of who has access to what

You have to restrict who has access to your IT systems and buildings – you can't let just anyone in unaccompanied because this will leave your systems vulnerable. The fewer people with access, the better. Visitors should be clearly identifiable. Make sure you limit IT access to people who work for you, where possible.

10. Don't keep data for longer than you need it

Staying on top of what personal data you hold will save you time and resources. It will also help you with your data protection responsibilities. Only keep what you need, for as long as you need it.

11. Dispose of old IT equipment and records securely

Before you get rid of them, make sure no personal data is left on personal computers, laptops, smartphones or any other devices. You could consider using deletion software, or hire a specialist to wipe the data. This will ensure no one can access information they're not supposed to see when you dispose of the equipment.