5 WAYS TO PROTECT YOUR DATA - A GUIDE

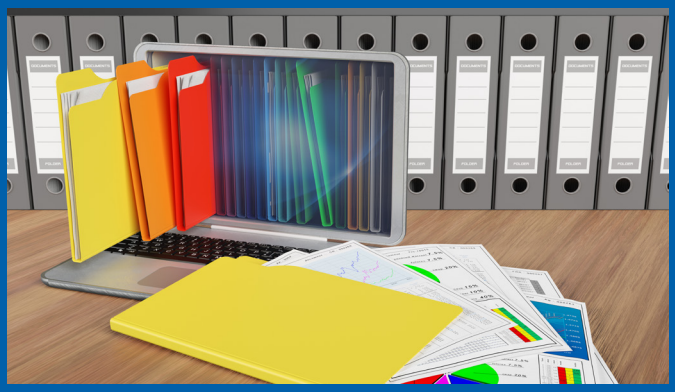
Have you ever lost a file? Had a hard drive fail at home, loosing precious memories and moments? How did you feel, the devastation of no longer having those moments when your parents celebrated their Golden Wedding Anniversary, or your hike across America, wiped out without a care? Did you have a backup in place, or at least think you did, but that failed too?

In schools when this happens, it can be devastating, on more than a personal level. The safe storage of data is integral to the efficient running of a school. It is essential to know how to ensure a backup is in place and check that it is running successfully; to train staff to recognise unethical emails and so on. Read more for our 5 top ways to protect your data at work.

WHAT'S IN A BACKUP?

What it does:

A backup does exactly as it says on the tin - makes a backup of your files or programmes dependent on what you specify.



What types of backup are there?

Cloud - where all your files and data are backed up to a safe storage area on the internet via a managed server software provided by your IT Partner.

On-Site - typically housed in the server room of your school, where each day, your files are backed up. Periodically a back-up can be carried out onto a separate server, still within the building, or to the cloud in a hybrid solution.

Off-Line - a physical hard disk which is exchanged each day, with the backup being stored on site in a fire-proof safe.

ANTI-RANSOMWARE

What it does:

Anti-Ransomware is another thing that does what it says! Running continuously on your PC, server and other devices, it will monitor for any tampering with your files and prevent them being encrypted with ransomware.

Why you need it:

Anti-Ransomware is a must for busy schools and colleges, as you cannot constantly monitor everything that your staff are doing, what they are clicking on etc. In the unlikely event of a hacker getting through with ransomware, the software holds previous versions of your data to re-install over the infected files. This is done automatically with the ransomware being removed seamlessly.

PATCHING YOUR DEVICE

What it does:

Software developers are constantly finding ways to prevent hackers compromising their programmes and apps. When a new 'patch' is created by a developer, it is sent to all their users, to be downloaded onto their devices to prevent hackers gaining access to the systems.

Why you need it:

By patching your device, you are installing the latest system software; anti-ransomware; bug fixes and so on for each programme, app or operating system. If you don't carry this out, then hackers are more likely to access your device as you haven't 'patched' the latest hole that they are using to get into your cyber world.

USER TRAINING

What it does:

By keeping your staff trained on cyber threats, you are creating a strong barrier to intrusions.

How to roll it out:

The National Cyber Security Centre provide advice and training along with their 'Exercise in a Box' initiative that each member of staff can do from their desk. Visit www.ncsc.gov.uk for more information.

ENCRYPTION

What it does:

By encrypting your device, you are creating a virtual lock, so that in the instance that your device might be stolen, all passwords and communications are virtually impossible to hack without the virtual key.

By using a managed encryption service, if you loose your key, the data is still accessible to you.

Why you need it:

If you leave your laptop on the train, or in the backseat of your car, and it is taken, the hard drive will be useless to the thief, as the encrypted files will prevent your data being accessed.

Call us to discuss your protection:

01787 221166
hello@cablers.co.uk
www.cablers.co.uk