Windows 4-Point Plan

Introduction:

We all know that we need to prepare our cars for winter, in the same way we need to prepare our devices (not for winter, though!), particularly our Windows devices, to be in good condition and be ready if the worst happens. Below is my 4-point plan to keep your machine in tip-top condition.

1: Backups:

Ensure you have a backup regime so you do not lose any of your documents or precious memories, such as photos. There are local, online, or both system options to choose from.

Local:

This can be a memory stick, though they have limited capacity. The better option is to use a separate portable Hard Drive (HDD), or a Solid-State Drive (SSD)

Methods:

a) Manually move files to the local drive at regular intervals

*Use the backup storage device and manually copy and paste (**not move**) from your internal drive to the backup drive. Remember to do this regularly, as the data is only as good as the last backup.*

b) Use the Windows built-in feature ‘File History’

Hold down the WIN key and press the I key (i), this opens up the settings. Search for ‘File History’. Follow the instructions, which start with ‘add a drive’. The computer will configure the drives to make regular backups. Remember that the backup should not be on the same computer as the original files.

Online:
There are several online backup systems available; the one you use day to day depends on your needs. They all offer some storage for free, but charge for additional storage. You can pick from Microsoft's OneDrive, Google Drive & Google Photos, Dropbox, and Mega, plus many more, and it depends on what suits you best.

Google Account Holders
Google Photos can be used to auto-upload Photos and Videos only
Google Drive can be used to auto-upload any file

Microsoft Account Holders: (If you have a Windows device, you already have a Microsoft Account; it is your email address and password.)
OneDrive can be configured to auto-upload any file (up to 2GB if you are a 365 subscriber)

Mega: Create an account at www.mega.nz and manually upload your files, or set up MegaSync to back them up. This system gives the most free storage before a charge is required.

Dropbox: Set up an account on the web using your normal email address and a password. Download the desktop client software and run it. Any files deposited in the Dropbox folder on your computer will be automatically uploaded to the cloud. After that, the files will be synchronised to all your other devices with Dropbox installed. There is limited free storage, and additional storage incurs a cost.

pCloud: www.pCloud.com Is a storage device similar to Dropbox, but gives more storage space for free, with a cost for larger amounts

Proton: www.protondrive.com is another online storage system, which could be

2: Maintenance:
Make sure you have some Anti-Malware software running and up to date. There is no need to pay for antivirus, as there are systems built into Windows itself.

Some years ago, the recommended method for virus protection was third-party software, such as AVG or Norton, because the built-in Windows Defender was not as efficient as it could be. However, Microsoft has improved Defender, so it is now the recommended antivirus and is free. Additionally, it is recommended to use a 3rd-party tool such as Malwarebytes as a secondary scanner, alongside the built-in Windows feature, “Malicious Software Removal Tool” (MRT). However, this is not an app and must be run manually. Windows has also got a built-in maintenance system to help clean and keep the PC running smoothly.

Defender:
This is enabled by using WIN key + I key (i) and Windows > Update & Security > Windows Security > Open Windows Security> check the various options for attention or not.

Malwarebytes:
This software is known to detect malware that Defender may miss.
Download the software from https://www.malwarebytes.com/mwb-download. When searching, be careful to select the correct site; the top results on the list are sponsored links.
Install the software and run it; it will ask you to do a free trial. Say yes, and then after the trial, it will send an advert and ask you to pay. DO NOT PAY; go to the 'continue with free option. (You will get adverts now and then.

Microsoft Malicious Software Removal Tool:
Type MRT in the search bar at the bottom-left of the screen > run MRT as an administrator; in the dialogue box, press YES, then press NEXT, and choose Quick or Full Scan.

Maintenance:
Type 'Maintenance' in the search bar and choose from the list of functions to run.
Type 'Health' in the search bar and press on Device Performance and Health, where you can inspect a report of your computer's health.

There are also third-party apps that can help you improve performance and clean up your computer.

CCleaner: An app that scans your computer and does a cleanup. It also has a few other features, such as a software uninstaller and registry cleanup. This can be downloaded from the Microsoft Store. Ensure you click the correct one; there are other similar apps. Periform makes it. Plus, when installing, be careful because sometimes another app can slip in, and you can install that by mistake. (An Avast version of Chrome is just one of them)

Bleach Bit: This also scans and performs cleanup. This is a bit more comprehensive and offers a few options, though the defaults are usually the best. This can be downloaded by searching for BleachBit online, but only download the version from bleachbit.org.

3: Recovery:

Ensure that a recovery system is enabled. So, you can reset to factory settings in case of a disaster and clear the whole machine.

Restore Point:
The restore point is so that the computer can revert back to its old state if an update or software has corrupted something and won't run properly. Sometimes these are created automatically; others require manual creation.
How to create a restore point: Type 'Restore Point' in the Search Box (bottom left). When the dialogue box appears, press Create a Restore Point.
How to Revert to a Restore Point: Use the same dialogue box used to create the point.

Recovery:
The computer can be restored to factory settings, with the option to keep your data or wipe it.

Reset Windows: Type 'Reset' in the search box (bottom left). Press ‘Reset this PC’; you'll see a few options to choose from. Pick the one that's most appropriate for your needs.

4: Passwords:

Throughout my time working with tech devices, the most common issue I have encountered is lost or forgotten passwords. However, there are ways to store your passwords securely so that you will never forget them.

The various methods:

Written on pieces of paper: Not a good idea; they usually get lost.

Written down in a notebook: Better than paper, has the advantage of all passwords in one place, but if it is stolen, the thief has your passwords, and you do not. If you have a fire/flood, then you do not have your passwords either.

Stored on the device itself: Your device can also store passwords; however, if your phone is left unlocked, anyone can view your passwords with a few keystrokes on both Apple and Android.

Stored in the Browser: The browser can also store passwords and autofill apps for you; again, the passwords can be seen by a few keystrokes if left open.

Stored in a Password Manager: This is the recommended method of storing passwords. The Manager is a 3rd-party app installed on all your devices, which are synchronised. Several password managers are available, with both free and paid options, but Bitwarden is the recommended one. On Windows, Bitwarden is protected by a single master password, which you must remember. Once set up, it can be protected on phones and tablets using your device's login PIN or biometrics (e.g., fingerprint). Do not forget this password; although there are ways to recover it, they are not easy.

Passkeys: A relatively new method for securing access to a device. It creates a system where locking your device also lets you enter your passwords in the correct application or website. This is a relatively new approach to account security, and over the next few years, it will become the de facto standard because it is considered more secure than passwords.

Summary:

Although these instructions refer to a Windows PC, the apps and software can also be installed on phones and tablets; even Windows Defender has a mobile app.

It is purely a personal choice whether to take action and maintain your device, using whichever method suits you. Still, please do; I know lots of people who have lost data in the past by poor computer management.