16 May 2019

TECH SNIPPETS

Information, Communication & Technology

In this issue:

The 3-finger salute

Holding down the ***Ctrl***, ***Alt*** and ***Delete*** keys together is often referred to facetiously as Microsoft's 3-finger salute. This is probably how you used to bring up the login screen when you settled down to work on a PC, but it is not usually required with Windows 10.

Once logged on to a PC though, the 3-finger salute still serves a useful function by offering the following options:

* **Lock** - Clicking on this option with your mouse, or simply pressing the ***Enter*** key, will lock your PC and prevent it from being used by anyone else. This option is not usually available on a shared PC for obvious reasons.

* **Sign out** - Use this option instead of right-clicking on the Windows icon at the bottom left of your screen (then choosing "**Shut down or sign out**" and then finally clicking on "**Sign out**").

* **Change a password** - Select this option to change your Windows login password. You will, of course, be asked for your "**Old password**", which is the one you used to login to start your current session. You will also be required to confirm your new password to rule out the possibility of any typing errors on your first attempt. Remember that passwords are case-sensitive. If you have the ***Caps Lock*** on then you will receive a warning of this just above the **Cancel** button at the bottom.

* **Task Manager** - Selecting this option opens the **Task Manager** app. You can also open the **Task Manager** by right-clicking on the taskbar at the bottom of your screen and choosing "**Task Manager**". If one of your open applications seems to have hung, or if you want to know why your PC seems to be running slowly, **Task Manager** is the place to go. It allows you to close hung applications and monitor your PC's processes and performance so you can maybe figure out what it is up to. More advanced users can also disable start-up apps and configure and control services running on their PCs.

News flash

Beginning with Windows 10 version 1809, you can now remove a USB flash drive whenever you feel like it without first having to eject it - unless you are writing files to it, of course.

In earlier versions of Windows, the default policy for handling external media was called *'Better performance'*, which necessitated having to safely eject a USB flash drive before you pulled it out of your PC's USB port.

From version 1809, *'Quick removal'* is the new default for all drive formats, keeping the device ready to remove at any time without using the **Safely Remove Hardware** process.

Network Security

There are growing concerns about the security of data on our school network. There have been several incidents in recent weeks where students have gained access to data they have no right to access, or have made use of staff accounts with or without the knowledge of the staff members concerned. Such incidents compromise the security of our marks databases, potentially allow students access to other privileged data, and can also allow them to bypass restrictions placed on them but which do not apply to staff. These breaches in security centre around classroom PCs (and laptops) and teachers' network accounts, but could also affect office PCs and administrator accounts unless all staff are alert to the risks.

Please observe the following protocols:

1. ***Never*** leave your classroom or office PC (or laptop) unattended and logged onto the network with your account without locking it before you leave. Use the 3-finger salute to bring up the **LOCK** option, then press the **Enter** key. Do not rely on a screensaver password to lock the PC for you - if one is set, it will only activate after several minutes, giving a mischievous student plenty of time to make use of your account in your absence.
2. In addition to locking your PC, lock your classroom or office door if you need to leave the area even for a short time. Your return may be delayed, giving that same mischievous student every opportunity to slip in and make some changes to marks or gain access to confidential information like upcoming exam papers.
3. ***Never under any circumstances let a student use your PC***. Doing so will set a precedent and give other students the impression they can do the same not just with your PC but also with any other staff members'. There are almost 100 PCs available in the Computer Centre and Media Centre for students to use. You can book the Computer Room or Blended Learning Room if students need to use a PC to do a class presentation. Alternatively, get them to bring their own laptops to school.
4. Do not save confidential data on a flash drive, external drive or even the PC's own internal hard drive. A portable drive can be "borrowed" temporarily by that same mischievous student, who can then make a copy of its contents. If the PC or portable drive is stolen, data written to it will be compromised. Save data on your S: drive or in the cloud instead.
5. ***Never*** allow students to watch you type your password, and of course ***never*** give it to them so they can log onto your classroom or office PC. If there is even a slight possibility that your password has been compromised, change it immediately.

We will shortly be changing our password requirements for staff. This will require passwords to be at least 8 characters long and also meet certain complexity requirements:

1. Passwords cannot contain the user's Account Name or Display Name.
2. The password contains characters from at least three of the following categories:

   •Uppercase letters of the alphabet
   •Lowercase letters of the alphabet
   •The numbers 0 through 9
   •Non-alphanumeric (special) characters, i.e. ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/