Security risks in Windows 7

Microsoft officially ended support for Windows 7 in January 2015 and extended support finally ended last week on Tuesday 14 January 2020. This means that Microsoft are no longer releasing security updates to keep Windows 7 devices safe and the best way for all students to stay secure is by using Windows 10.

If you are still running **Windows 7** on personally owned devices we advise you **NOT** to connect such devices to the Middlesex network, as this will open you up to the following risks.

Vulnerability to malware, viruses and Ransomware that may:

- Damage, delete or steal data
- Steal personal and financial data
- Spy on personal activity without your knowledge
- Ransomware designed to block access to your computer system until a sum of money is paid

To minimise risk from the vulnerabilities listed above, it is strongly advised to:

1. Upgrade personal Windows 7 devices to Windows 10 as soon as possible
2. Stop making any financial transactions such as internet banking or online shopping from a Windows 7 device
3. Stop using email (sending or receiving) on a Windows 7 device
4. Stop connecting Windows 7 devices to the Middlesex network or any Middlesex University online services, be it cabled, wirelessly or via a VPN

Windows 7 devices will be blocked from connecting to Middlesex networks in the near future so please update to Windows 10 as soon as possible.

More information will be forthcoming in the near future.