User Responsibilities and assertion

The NECS Use Your Own Device (UYOD) Virtual Desktop Infrastructure (VDI) remote access solution must **only** be used in the following way:

- From the user's home - provided a current up to date manufacturer-supported and patched operating system (eg Windows 10) and appropriate, fully functional anti-virus, anti-spyware and firewall software products are installed on the PC/laptop. One of Windows Defender or Sophos Home is required.

NB: Users must not use this remote access solution from any public areas such as internet cafes, public WIFI areas, hotel/train broadband connections etc.

- It is the users' responsibility who asserts that by using the UYOD VDI remote access solution that they have the above measures in place. NECS are employing security controls which will perform an integrity check of connecting devices to ensure they are patched and adequately protected. These require the user to install the security application OPSWAT on to the connecting device.

- The reason for this requirement is to safeguard and minimise the risk of malware such as 'key-loggers' or 'screen scrapers' that could otherwise be present on the device used to access the NECS infrastructure. If present, malware such as this could lead to compromised access credentials for clinical platforms and/or the unauthorised leakage of clinical data.

- The user is responsible for maintaining their home working environment in conformance with the practice's requirements for home working such as, but not limited to, Health & Safety, Display Screen Equipment (DSE) assessments, manual handling, fire safety, security of the premises, insurance, other individuals who have access to the area where the remote access is taking place, etc.

By using this platform you agree to the responsibilities outlined above.