LSHTM Information Management and Security Policy

Supporting policy: Bring Your Own Device Policy

Document Type	Policy
Document owner	Phil Rogers, Head of Information Security & IT Compliance

3.1.1 Virtual Desktop (**Recommended**)
To enable remote working on personal devices (that comply with the BYOD Configuration Requirements in this policy) the virtual desktop service, Horizon is provided. This grants access to LSHTM resources including a suite of applications in a familiar Windows environment. The virtual desktop can be accessed via this link: https://horizon.lshtm.ac.uk This service ensures LSHTM data remains under LSHTM control (and not on personal devices) while increasing the availability of LSHTM resources.

3.2.2 Install LSHTM Security Software (**Avoid if possible**)
To prevent data breaches from the loss of personal devices, J0 Tc ien

x Users must understand what data will be lost in the case of remote wiping.

x Cloud backups (e.g. iCloud on Apple devices) must not include LSHTM data.

x Never stored LSHTM data on personal storage devices (e.g. USB sticks, external drives etc.)

x Never use personal storage device with LSHTM controlled devices.

x All devices must have appropriate anti-virus installed and configured if available. ITo(t)-1 (r