Guidance for schools – using personal devices when working at home

Due to the effects of COVID-19, many schools are requiring staff to work from home for days or sometimes weeks at a time to avoid the risk of infection. If staff are required to carry out work using a device such as a laptop, where possible this should be carried out using a Trust or school owned device that is managed and maintained by the Trust/school. However, it is recognised that, in these unique times, schools may not have a sufficient number of devices to support the volume of staff required to work from home at any one time. Therefore, in exceptional circumstances, staff may be given permission to work on their own devices. **This should be avoided where possible, and should only be a temporary measure.**

Working from home may require the need to access personal, sensitive and/or confidential information. This may be via the Internet on a cloud-based system, i.e. Outlook 365, Arbor, or via documents stored on the school's server and hard drive. The legal requirements under GDPR to protect this information still apply regardless of the working circumstances, so it is imperative that all reasonable steps are taken to fulfil this obligation. The actions below are required for all staff working from home using a personal device to promote effective information security. Headteachers are advised to issue this guidance to their staff as an addendum to the Acceptable Use Agreements already in place in their school, and ensure that staff understand and agree to abide by it.

For the device:

- Password protect your device, so that no-one can start it up and access it without the password or pin code. Ensure you use a password that is complex enough not to be easily guessed.
- If the device is shared, i.e. used by more than one person in your household, set up separate user accounts so that each user has to log on with their own name and password.
- When the device is not in use, either shut it down or lock the screen so that no-one else can use it.
- Ensure that all Windows programmes and other software that is installed on the device are regularly updated.
- Check that the Wi-Fi home router your device is connected to has its firewall enabled, is set to private and that the local Wi-Fi key is secure.
- Install an appropriate anti-virus software, and make sure it is active and regularly checking your device.

For accessing cloud-based systems or accounts: (i.e. Outlook 365, Arbor)

- Don't save the link to any site that contains personal, sensitive or confidential information to a bookmark or favourites page.
- When you have finished working on a system or no longer need to access an account, make sure to 'log off' and don't just exit the page by clicking on the cross.
- Don't auto-save passwords; you should be typing in the password each time that you require access.
- Don't download or save any documents, pictures or data that contains personal, sensitive or confidential information to your personal device
- If data or document do need to be saved, use cloud-based storage such as One Drive or Google Drive.

For general use:

- Don't use passwords that are also used in your personal life or are known/used by your family – make any passwords used for work purposes different to those you use for non-work purposes.
- Only log on to a private Wi-Fi connection that is password protected; do not use open or public Wi-Fi connections.
- If you are using a memory stick, or other form of external hard drive, make sure it is encrypted or password protected.