

# HOME WORKING GUIDELINES

## How to keep your data safe while working from home

Many of us undertake some form of home working, whether routinely working remotely, or just checking our emails occasionally. Whilst we are working from home, particularly if using personal devices, we remain responsible for the security of our data and the privacy of our students and stakeholders. Here are a few top tips to help you safely navigate home working:

### 1. Check your device

If you are using a personal device whilst working from home, you are responsible for making sure that it is free of any viruses or malicious software that may infect the school network. You should ensure that your device is fully updated and protected by anti-virus software, and you must run a virus scan before accessing any school systems or information.

### 2. Browse securely

If you are connecting to a home wifi network, you should ensure that this is securely set up with password protection. You will need to use the school VPN to access some college systems or when connecting to a public or unsecured (i.e. no password required) wifi network. However, we recommend that you use the school's VPN at all times when accessing school systems and information offsite, for an added layer of security.

### 3. Use your school accounts

Be sure not to confuse your personal and work accounts whilst using personal devices. Work related correspondence must only be conducted through your school account and college documents and information must only be stored on school systems, such as Office365.

### 4. Remain vigilant

Cyber security threats can affect you at home as well as in the office; a virus affecting your personal device can in turn affect your work account and the wider school network. Whilst working from home, remain vigilant against phishing emails, both on your work account and any personal accounts.

### 5. Store securely

If you need to take paperwork home from the office, this must be stored securely and returned to school as soon as possible. School documents must not be disposed of in personal waste.

School documents and information must be stored on school systems, and must not be stored on personal devices. If you need to temporarily store documents on your device, be sure to erase them from your device at the end of the day.

### 6. Report breaches

If the worst comes to the worst and data or devices are compromised or lost while working from, report it to the Data Protection Officer immediately.