Working from home

Guidance for remote working during the Coronavirus (COVID-19) pandemic

During the ongoing Coronavirus (COVID-19) Pandemic, you'll be aware that more and more staff are working from home. Whether you are now doing some or all of your work from your home, it's important to remember that you are still working with personal information- some of which may be considered 'special category'.
Consider your home as an extension of your office, and follow these tips to ensure your colleagues', students' and your personal data stays as safe as possible:

- Avoid using Public Wi-FI, use a home network or hotspot instead.
- Never leave your laptops, phones or paperwork in your car overnight. Keep them in a safe place, locked securely in your home.
- Be aware of your surroundings – can someone see your screen through a window? Can your family access, view or overhear anything sensitive?
- Avoid leaving drinks or food on or near schoolwork, paperwork or laptops – if it spills it could destroy information you and your students need.
- Don't send any work to or from your personal email address. It does not have the same level of security as your School's systems and may put personal data at risk. Use headsets or headphones during Skype meetings or phone calls to prevent family or neighbours overhearing something sensitive.
- Don't throw paper files with personal information in your rubbish or recycling bins. Shred with a cross-cutting shredder, or keep it securely until it can be returned to the school to destroy.
- Only use USB sticks if they come from the school, and you know that you are allowed to use them.

If you are using a personal mobile phone or laptop for work:

- **Make sure that it is password protected.** Make sure the passwords are long, strong and unique: at least 12 characters that are a mix of numbers, symbols and capital and lowercase letters.
- **Make sure your devices have up to date anti-virus installed, and that all software updates are completed.** This ensures that security updates are in place and you are less vulnerable to cyber criminals.
- **Change the default passwords on your Wi-Fi router and any other devices connected to the internet (e.g. Alexa or Google Home, baby monitors).** This makes it much harder for unauthorised people to access them and gain your information.

Suspicious Links
As always, try to avoid clicking links in emails, text messages or Whatsapp wherever possible, and especially if something doesn't seem right. Clicking on a bad link in a "phishing" email or text can lead to malware infections and loss of data including stored passwords.

Unfortunately, cyber criminals are particularly likely to try to take advantage of the worry surrounding the virus, so be especially careful that you don't panic, and think before you click!

If you spot a suspicious text, message or email, report it to your IT provider immediately.

Here are some tips on how to spot a phishing message:

- Does the message have poor grammar, punctuation and spelling?
- Is the design and overall quality what you'd expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to you as 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet.
- Is it asking you to provide personal information in an email? No official organisation will ask you to do this.

If you click on a link in a potential phishing scam, don’t panic! Take these steps:

- If you have been tricked into providing your password, change all passwords.
- Report the possible scam to your IT department and follow their guidance.
- If on a personal device open your antivirus software and run a full scan, follow any instructions given.
- If you have lost money as an individual you must report it as a crime to Action Fraud by visiting www.actionfraud.police.uk

Finally, if you need any advice about information security while working from home, please contact the individual in your School responsible for data protection, or Veritau Ltd (your School’s Data Protection Officer) at SchoolsDPO@veritau.co.uk

Veritau