Guidance Note For Staff On Working From Home

- Be Vigilant – No one in your household should have access to or see the personal data you are using
    1. Be aware of your surroundings and who may be able to view your screen/work.
    2. Do not write down your passwords on paper where they can be discovered.

Use strong passwords to protect your work devices and make sure you use a password that no-one else in the household knows or can guess.

- Remember your data protection training to help you to ensure that everything is kept safe whilst at home. Protecting student and staff data must remain the highest priority. Data breaches can cause real and significant harm to individuals and the risk of data breaches become much higher when data is accessed remotely or on a portable device.

- Ensure that you use devices provided by the college rather than your own device to access the college's network
  Own devices should only be used with agreement from the IT team. This will help prevent unknown risks to the college's network (such as malware or security breaches). In addition to this: -
    1. Check that your device is fully up to date with anti-virus, firewall, malware and security updates.
    2. Ensure that work documents are saved on the college network securely rather than on the desktop or in "my documents."
    3. Ensure your device has a password or (for tablets/phones) pin code. Passwords should be complex (a mixture of numbers, letters and capitals).

- Lock your screen while you are away/not using your device. Please be vigilant to lock screens when not in use for long periods or where you are stepping away from your device. In addition, devices should be shut down at the end of the day.

- Ensure that college IT equipment is kept in a secure place. It is your responsibility to ensure that college equipment is kept secure (for example in a locked draw). If a device becomes lost or stolen, please report this to the college without delay and within 72 hours.

- Do not use your own USB memory sticks and plug them into college devices to take data from college systems or to upload data or documents to college systems. This goes for memory sticks, pen drives and external hard drives. They should not be plugged into college devices unless they are issued/approved by the college IT team.

- Do not install or download any software onto a work device without the approval of the college. Where approval is given, they should also be virus checked before they are downloaded onto the college's systems.

- Ensure that if you are communicating remotely via video conferencing with your colleagues or learners that:
    1. You use platforms which have been approved by the college.

2. Ensure that webcams are only activated when they need to be.
3. Do not record unless authorised to do so by the college (and the participants to the call also consent).

- Always be careful which websites you visit and which emails attachments you open.
    1. Be careful when opening attachments to emails - even if the message appears to be from someone you know. Email attachments infected with viruses are one of the most widely used methods for infecting PCs.
    2. Be vigilant against phishing attacks claiming financial rewards or encouraging charity donations. Phishing emails can look like they came from a real company or person you know and trust. The sole purpose of a phishing email scam is to trick you into going to a fake website that looks equally authentic and inputting personal information that would in turn provide the criminal with access to your accounts.
    3. Remember that text, music and other content on the internet are copyright works. You should not download or email such content to others unless certain that the owner of such works allows this.

- Ensure not to give out your personal details, such as a mobile phone number and personal email address to learners. Do not use personal email accounts or numbers for college use.

- Ensure you keep your own shared area and own email accounts organised.
  Do not keep emails or documents for longer than you need and it is each individual's responsibility to ensure their accounts are organised appropriately. If necessary, check the college's retention policy and schedule and ensure that you are complying with it and not storing personal data longer than you are allowed to.

- Paper records count too
    1. Paper documents taken from college or printed off at home must be kept secure at home just as they would be at college.
    2. At the end of the working day, or when you leave your workstation unoccupied, all paper documents containing personal information need to be securely locked away to avoid unauthorised access.
    3. You must ensure that documents are returned to secure storage at college as appropriate or they are destroyed securely at home. (see college's retention policy).
    4. Do not put confidential waste into the ordinary waste. Ensure that it is shredded first.

Do report any breaches of the above to your line manager who will refer to our IT Acceptable use policies. Thank you.