Working from home – Top tips to protect data

Like many organisations, the Society has a hybrid model of working for support centre colleagues. It is important to remember some key principles when working remotely or from home.

The following ten tips are adapted from the ICO's working from home guidance:

1. **Follow our policies, procedures and guidance**

   Our policies have been developed to ensure that data is adequately protected. Avoid the temptation to do things in a way you think is more convenient, such as sending emails through your personal account or using the video conferencing app that you use with friends for work calls.

2. **Only use approved technology for handling personal data**

   If you have been provided you with technology such as hardware or software you should use it. This will provide the best protection for personal data.

3. **Consider confidentiality when holding conversations or using a screen**

   You may be sharing your home working space with other family members. Try to hold conversations where they are less likely to overhear you and position your screen where it is less likely to be overseen.

4. **Take care with print outs**

   At the office, it is likely you can use confidential waste bins. At home you won't have that facility. You should keep printing of confidential documents to a minimum. Where it is necessary to print confidential documents, make sure they are stored securely and are shredded if no longer in use. Papers that cannot be securely disposed of should be secured until they can be returned to the workplace for secure storage or destruction.

5. **Don't mix the Society's data with your own personal data**

   You should have been provided with Society equipment, which should be used for work purposes. In the exceptional circumstances where you have to work using your own device and software, keep your organisation's data separate to avoid accidentally keeping hold of data for longer than is necessary.

6. **Lock it away where possible**

   To avoid loss or theft of personal data, put print outs and devices away at the end of the working day if possible.

7. **Be extra vigilant about opening web links and attachments in emails or other messages**

Don’t click on unfamiliar web links or attachments claiming to give you important coronavirus updates. In recent years there has been a rise in scams and phishing attacks.

8. **Use strong passwords**

Whether using online storage, a laptop or some other technology, it’s important to make your passwords hard to guess. The NCSC recommends using three random words together as a password (eg 'coffeetrainfish' or ‘walltincake’). Make sure you use different passwords for different services too.

9. **Communicate securely**

Use the communication facilities provided to the Society, where available. Stick to the usual rules when sharing information with third-party organisations, eg, encrypting attachments and verifying recipients’ details. Where using email, consider password protecting documents and sharing the passwords via a different channel, like text.

10. **Keep software up to date**

If you’re using your own equipment, don’t be an easy target for hackers. Keep your security software up to date to make it more difficult for them to get in.