ONLINE SAFETY TIPS

1. Choose, use and protect your **passwords** carefully, and use a different one for every online account in case one or more get hacked. Best advice is to use three random words, not family, friends or pet names, use a minimum of 8 characters, try to maximise use of characters and symbols – NEVER DISCLOSE YOUR PASSWORD.

2. Look after your **mobile devices**. Don't leave them unattended in public places, and protect them with a PIN or passcode.

3. Ensure you always have **internet security software** loaded on computers and a similar app on your mobile device, and make sure that this is kept updated and switched on. Remember that smartphones and tablets can get compromised as much as computers. **Apply patches and updates** as soon as possible once notified that they are available, this will ensure minimal vulnerability to software.

4. **Back up data** - The information held on your computer may be irreplaceable. Regularly backing up your data will ensure that you have more than one copy, two principal methods are the use of 'online (cloud) storage', or 'portable hard drives' (can be stored off site for additional security), other methods such USB memory sticks are not recommended as they can easily be lost or stolen.

5. Never reveal **too much personal or financial information** in emails, on social networking and dating sites and in person. You never know who might see it, or use it.

6. Always consider that online or on the phone, **people aren't always who they claim to be**. Fake emails and phone calls are a favourite way for fraudsters to approach their victims.

7. **Don't click on links in emails**, posts, tweets or texts – and **don't open attachments** – if the source isn't 100% known and trustworthy, or it seems strange that you'd be receiving them.

8. Never pay for anything by **direct bank transfer** – including goods, services, tickets, travel and holidays – unless it's to someone you know personally and is reputable.

9. You must not assume that **Wi-Fi hotspots** in places like cafes, bars and hotel rooms are secure, so never use them when you're doing anything confidential online. Instead, use 3G or 4G or if it's for work, a VPN (virtual private network).

10. Take your time and **think twice**, because everything may not be as it seems - if something seems too good to be true, it probably is.

IF YOU ARE UNSURE OR SUSPICIOUS, **STOP**, **THINK,** AND REMEMBER:

'DON'T BE TEMPTED, DON'T BE RUSHED, SEEK ADVICE FROM SOMEONE YOU TRUST'

Further information can be found by visiting: **https://www.getsafeonline.org**

https://www.cyberaware.gov.uk

Please help others by reporting any Cyber Crime through the National Reporting Mechanism:

http://www.actionfraud.police.uk Telephone: 0300 123 2040