SAFETY ON THE TELEPHONE

• Never agree to anything over the phone. Don't be shy of just hanging up on telephone cold callers.
• Never reply to unsolicited text messages, even to try and stop them. Just delete them.
• Never give any personal information over the phone unless you made the call and are certain of who you are speaking to.
• Use a password, passcode or pattern code to lock your phone.
• Don't store password reminders on your phone.
• Don't open suspicious or unsolicited messages.

Register your mobile with www.immobilise.com,
using your IMEI number (15 to 17 digit code
usually behind the battery - or key in *#06#).

If your phone is stolen, report it immediately to the police and your service provider to block usage, even if it's pay-as-you-go.
Don't report lost phones as stolen. This is a crime.

If you have a smartphone

• Install anti-virus software specifically designed for mobile phones. Ask for advice at the store where you bought your phone.
• Avoid opening links or downloading games and apps unless you are certain of their source.
• Clear your browser history – especially if using online banking.

Remember:

If you have a smartphone,
take the same precautions
as you would when accessing the
internet over any other device.

Be careful with your location settings.
If you use your phone to update social media or to upload photos, location data could be uploaded to the internet without you realising. Burglars can use this information to find out where you live and even when you are likely to be out of the house.
If you are unsure, ask a member of staff at the shop where you bought your phone to show you the location settings.

Sign up to the

Telephone Preference Service
www.tpsonline.org.uk or 0845 070 0707
and the Mail Preference Service
www.mpsonline.org.uk to minimise
unsolicited calls and mail.

Stay safe from scams

Remember: scammers often pretend to be from legitimate, well-known, national or global companies like banks or utilities providers. If in doubt, hang up and phone the company yourself, using a phone number from their official website, Yellow Pages or letterheaded correspondence from them.

A common scam involves someone calling you up and claiming that there is something wrong with your computer and they can fix it for you. This is a hoax.
If you think there is a problem with your computer or you want to buy or update antivirus software:
• Ask advice from the store where you bought it.
• Ask a trusted computer repair technician that you have contacted yourself.
• Never give control of your computer remotely to a third party over the telephone.

The Metropolitan Police produce a useful online booklet called **The Little Book of Big Scams**. This can be downloaded at www.met.police.uk/docs/little_book_scam.pdf and an audio version is also available (visit www.met.police.uk and type 'little book big scams' into the search box). Two websites with useful information about hoaxes are www.snopes.com and www.hoax-slayer.com.h

Some scams or frauds involve online dating. Be very careful about what information you give to someone you have never met in person, and never send any money to someone you haven't met.
Scams can also revolve around job-hunting. As well as being wary of links and attachments in unsolicited emails, beware of interview, job or training 'offers' that require you to buy books or equipment, or pay a fee upfront

The charity 'Think Jessica' has an anti-scam website, www.thinkjessica.com, with a useful poster, FAQs and information about what to look out for, as well as further materials that you can order.