E-Safety @ E-Safety @ E-Safety @

St Andrew's CE Primary School, Yetminster

At St Andrew's CE Primary School we believe in keeping your child safe both in and out of school. Children today have embraced new technologies as a source of information, education and entertainment. The use of digital technology is regarded as normal by this generation, and it is now fully integrated into their daily lives.

Children and young people are using technology in new and exciting ways, enhancing and enriching their lives with the many tools on offer. In their exploration of these technologies, young people are not only developing their ICT skills, but also a whole host of 'softer' skills - creativity, communication and networking skills, for example - which will be much in demand by the employers of the future.

Children are increasingly referred to as 'digital natives': citizens born into a digital world, who grow up surrounded by and emerged in the technology and tools of the digital age. Their confidence and skills in using this technology is typically high, but their knowledge and awareness of the inherent issues, risks and dangers is usually very low.

Children and young people need to be empowered to keep themselves safe - this isn't just a top down approach.

Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim.

At St Andrew's CE Primary school, we have a specific e-safety curriculum that covers every group from EYFS to Year 6. The coverage of topics has been designed in line with CEOP, the THINKUKNOW website and from the training the Headteacher, staff and governors have attended. We also have a specific e-safety policy, an e-safety protocol for everyone working in school, a risk assessment that is regularly reviewed, a training programme for our teachers and teaching assistants on their online reputation and a dedication to ensure that children can explore the digital world through various devices safely.

Useful sites relating to E-safety

www.thinkuknow.co.uk
www.ceop.gov.uk
www.iwf.org.uk
www.stopcyberbullying.org
www.childline.org.uk
www.123people.co.uk
www.stopthinkdorset.co.uk
http://www.saferinternet.org.uk/ufiles/What-Can-I-Do-Right-Now---Checklist.pdf

The logo in the next column will take you to the CEOP website which is a great place to visit if you would like to know more: www.thinkuknow.co.uk Here you can report online incidents. Just look for the CEOP button or tab on our website and click for advice

BBC WEBWISE

THEY SHARE, BUT DO THEY TAKE CARE?

To make sure you don't share too much information online here are ten tips. Have a look at this video

1. Watch your back

Whenever you're about to post something online, pause and just imagine someone in authority, someone you respect, reading that post or looking at that photo. If that feels uncomfortable, don't do it.

2. Got a nickname?

Think about using a nickname instead of your real name if you're signing up to a microblogging site like Twitter. Consider setting up a separate, personal email account to use with social media sites, rather than using your work, or even your main personal email. Remember, only connect to people you know.

3. Check your settings

Use the privacy and security settings on social media sites so that only friends and family can see your pages. Then speak to friends and family and encourage them to tighten their privacy settings too as they could affect you. Even if your account is locked as private, personal information you have shared with others could still be accessed through their pages.

4. Mother's maiden name

Don't use your mother's real maiden name as a password or as a bank security answer. It doesn't really matter whether you use the real one so make up a name that only you know. Just make sure you remember it.

5. Guard personal information

Continue reading the main story

Mum Sarah and daughter Becky

Did another mother and daughter do any better in the online sharing test?

Don't post any personal information- your address, email address or mobile number - publicly online. Just one piece of personal information could be used by a complete stranger to find out even more.

If you want to include your birthday in your profile it's safer not to actually display it publicly - providing your full date of birth makes you more vulnerable to identity fraud.

6. Photos and videos

Be careful about which photos and videos you share on social media sites - avoid photos of your home, work, school or places you're associated with. Remember, once you've put a picture of yourself online, other people may be able to see it and download it - it may not just be yours anymore.

7. Check what's needed

Don't give out information online simply because it's asked for - think whether whoever is asking for it, really needs it. When you're filling in forms online, for example to register with a website or sign up for a newsletter, always provide the minimum information possible.

8. Direct message if you can

It's almost always possible to send a direct message or private message on social media platforms. If you're having a personal chat, this is the best option to go for - unless you don't mind sharing your conversation with millions of other users. Alternatively, send an email from a private account.

9. Delete old accounts

If you've stopped using a social media site or forum, then close your account down. There's no point in leaving personal information out there unnecessarily.

10. Get anti-virus software

Make sure you have anti-virus software installed on your computer and be careful what you download or install on your computer.