Cybersafety with Susan McLean

Thank you to all the families who attended the Cybersafety talk on Wednesday 9 May with Susan McLean. For those who were and were not able to attend, we have a brief summary of Susan's key tips.

1. **Talk about Cyber safety - Talk early and talk often**

Parents must learn about the internet with their child – get students to share their knowledge of the internet with their parents in a fun environment.

The internet and the various applications are a lot of fun and a wonderful tool……maximize the benefits and surf safely together!

Teach children that information on the internet is not always reliable.

Supervision

2. **Apply the same safety standards to the internet as you do in the real world. You wouldn't leave your child unsupervised in a physical public location so don't leave them unsupervised in a virtual public location.**

Internet connected devices should be in a common area of the house not in the bedroom.

Parental monitoring is vital – shoulder surfing - walk past and see what your child is doing.

Install filters and other monitoring/blocking software to minimise dangers. This is already done on the schools network but advised parents to have up to date filtering software installed on home networks and to protect all devices at home including the school laptop.

Susan recommends Family Zone: http://fzo.io/cybersafetysolutions and applying restrictions on smart phones under Settings.

Know your children's passwords.

Do not let young children 'google' or 'you tube' aimlessly with no supervision. Children need to be taught about search engines and how they work.

Social media

3. **Primary school aged children are not allowed to be on social media sites. Social media sites have a minimum age of 13. It is illegal for children under the age of 13 to be on these sites and apps.**

Parents should respect the rules of these sites and not create accounts for Primary school children or allow children to use your account.

Most sites have privacy features but many users do not enable them. It is recommended to turn on these privacy features on your own accounts.

Games

4. **If your child is playing online games it is your responsibility to make sure that you know how to play the game too in case of problems.**

Research the game by typing into Google: What is this game? Is this game safe?

Play online games together as a number of primary school children are playing violent games regularly.

Turn off the chat function as it can allow unknown adults to contact your child.

Photography and posting on social media

5. **Do not post photographs of other children on your social media without consent and your own children in identifiable uniforms or places.**

Think carefully about the digital footprint that is being created about your child.

Clubs and dance school and other activity based organisations must have policies about not posting photographs of children on the internet.

Problems

6. **Make sure that your children understand that they will not get in trouble if they tell you about a problem. Encourage them to talk to you or a trusted adult.**

Advise your student/child to immediately exit any site that makes them feel uncomfortable or worried. Basic protective behaviour principles apply.

If your child is contacted inappropriately, take a screen shot of the computer and advise school or police depending on the situation. Do not take matters into your own hands by responding.

Be aware of current texting codes

Smart phones

7. **Primary school children do not need smart phones.**

If they need a phone to be in contact with parents/guardians then provide them with a 'dumb' phone that can make calls and send texts. There are several phones available for this purpose.

Smart phones are not allowed in the school grounds during school hours. The SEPS Mobile Phone Policy states that students are not allowed to be in possession of a mobile phone on school grounds.

Apps

8. **Do you know about NQ Vault, KIK, Snapchat, Omegle, Instagram, Musical.ly, Yubo, Spot a Friend, Meet me, Sarahah, and Melon?**

These sites are known sites for predatory behaviour.

For example, Snapchat is fun and can be used safely with a parent. Snapchat has a mapping function that displays the device location publicly. Turn off the mapping function and turn off chat and it is a safer product.

Be Informed

9. **Susan has a Facebook page, which she provides regular updates of cybersafety issues**
10. **Susan McLean recommends using the Office of the eSafety Commissioners website for information about cybersafety.**
11. **If you have any queries or concerns about safety, you are encouraged to contact the Principal and School Council.**