Keeping Technology Use Safe @ Home

With the need for 'Learning @ Home' during the COVID-19 pandemic, technology use is increasing or changing for many people. Families are being asked to use technology in ways unfamiliar to them, and whilst many are coping okay and learning quickly, others find it daunting and need to be reassured. However, one thing is consistent with all, we want technology use to be safe. The following information has tips to help you keep technology use at home safe, and clarifies what measures the school has in place.

Devices supplied by the school . . .

- The school is very well resourced and has been able to provide IT devices to all students from Prep to Year 10.
    - Prep – Year 2: IPads
    - Year 3-8: School laptops retained by the school
    - Year 9/10: Laptops purchased by the students over a two-year period
    - There are IPads in Kindergarten, but these have not been sent home with students for the 'Learning @ Home' period.

- Each device is allocated to a specific student for tracking and servicing requirements.
- IPads are laptops are managed centrally by our IT manager

School provided security . . .

- Laptop functionality is centrally controlled by the IT manager, with many administrative functions locked down and unavailable to students
- Web content filtering and virus protection is managed through Sophos endpoint protection, which also provides coverage at home.

Some general tips for safe IT use . . .

- Always have children use devices in a public space where they can be supervised, like the lounge or dining room
- Don't allow children to have devices in their rooms, and store and charge devices overnight in a central location
- Never share personal information over the internet with an unknown identity or organisation.
    - Be aware that many online spaces are used with pseudonyms, and not real identities. So who someone presents themselves as may not be reality

    - Whenever asked for personal information, check the authenticity of the request (advice on this from the e-safety commissioner)
- If something questionable comes onto the screen, teach children to minimise the window, turn off the screen on a desktop PC or close the laptop and report the issue to a parent (don't turn the machine off or you won't know what the issue is)
- Have an open and honest agreement with your children about their access to technology. If they don't want you to have access to the device without them, you should be asking questions.
    - As a parent it is not a breach of privacy to want to protect your child from danger on a device

Further advice available from the e-safety commissioner . . .

- https://www.esafety.gov.au/
- https://www.esafety.gov.au/parents
- https://www.esafety.gov.au/about-us/blog/covid-19-online-safety-kit-parents-and-carers

Other options for IT safety advice . . .

Having heard Susan McLean present live I can attest that she is on the cutting edge of cyber safety matters. She is frank, holds no punches and will probably frighten you a little with the reality of cyber safety. Whilst she is not a confessing Christian, she does speak clearly about being ferociously discerning, and her biggest tip for parents is 'learn to say no!'.

She has some great books and her website is a fantastic resource.

http://www.cybersafetysolutions.com.au/

You have endless commercial options for protection of all your devices at home, so if you want to chat through options please feel free to get in touch with our IT manager, R Brouwer, or peruse the internet security overview he wrote for us some time ago.

You might consider:

- www.covenanteyes.com
- www.familyzone.com
- https://www.qustodio.com/en/family/how-it-works/
- https://support.apple.com/en-au/HT201304
- https://www.opendns.com/home-internet-security/