Prince Albert Community Trust
Online Safety Update
ISSUE 18
DECEMBER 17
WWW.PACT.BHAM.SCH.UK
@thePA_CT

PACT Prince Albert COMMUNITY TRUST

Buyer beware, in the race to market, some companies may have cut some corners when it comes to the security of their products

Tis' the season! Is your tech present safe and appropriate?

Toy manufacturers are betting on smart tech to invigorate their offerings to younger children this festive season. Products like the Furby-Connect, i-Que Intelligent Robot, Toy-Fi Teddy and CloudPets all offer Bluetooth connectivity and companion iOS and Android apps.

Unfortunately, all of the toys listed above fail to implement any sort of authentication on their Bluetooth connections, meaning anyone within range can install the companion app on their device, search and connect to the smart toy and start sending your child messages which the toy will blindly play through their built in speakers.

Even after a Which? investigation, the manufacturers that have responded have all stated that they believe their toys to be safe because it would be unlikely that anyone would want to hack the toys, and that they would need technical knowledge to pull the hack off.

The reality of this is that the technical knowledge required is only the ability to connect a smartphone to a Bluetooth device, a common procedure for most smartphone owners.

The big tech revolution for this year is the home speaker with integrated smart assistant. Leading the pack is Amazon with its Echo speaker, followed by Google, Microsoft and others. The idea being that you can use your voice to ask the personal assistant to give you information from your schedule or the internet, make lists, appointments, and ask it to play music. It can also control other smart devices such as heating and lights, you can even order products, all with your voice.

If you are considering purchasing a smart speaker, or maybe you have recently bought one, we suggest that you consider how the younger members of your family might interact with the device. The security on them will be sound, but be aware that your child could be able to access inappropriate content through one of these devices, or order things from the internet without your permission.

Taking Alexa as an example, the digital assistant doesn't have much in the way of parental controls, this is highlighted by the fact that if you have an Amazon device such as a Fire Tablet with the parental controls enabled, this disables Alexa voice control with no override.

As with everything in the fast moving tech world, it's going to take a while for legislation to catch up, for these new markets to mature, for manufacturers to be more aware of how the devices can be misused, and for the longer term impact of these technologies to be studied.

Indeed some countries are already starting to warn and legislate against unsafe devices, only last week the German regulator banned smartwatches aimed at children, describing them as spying devices, after it had earlier banned an internet connected doll called "My Friend Cayla".

Norway has also filed complaints against the doll and the i-Que Intelligent Robot, along with American consumer groups, and in July the FBI issued a general warning about connected toys where it stated, "Security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use".

Until UK consumer groups, researchers and government put pressure, guidelines and legislation onto this sector, it is down to us as consumers and parents to show disapproval for products that may be inappropriate, not have mature enough parental settings, or are just insecure, by not spending our money on them.

Our advice is to thoroughly research the products you are interested in before you purchase. Here are some questions you could ask to help you assess the safety of a product:

- Is the product appropriate for all members of your family?
- What parental controls does the product have in place?
- Could the product be misused either intentionally or unintentionally?
- What security measures does the product have in place?
- What impact could prolonged use of this product have?
- What do consumer groups and product testers say about the products?

We wish you and your family a happy and safe holiday time, and for more advice on the safe use of technology this festive season, read the related articles over the page and visit our PACT and school websites for more advice, links and resources.

Safer Internet Centre

For more advice on the safe use of technology this Christmas why not visit the UK Safer Internet Centre? Here you will find advice for young people, parents and education professionals.

Visit the UK Safer Internet Centre at:
www.saferinternet.org.uk/advice-centre

Online Safety in the News

Schools can't tackle online safety alone

Parents can often feel overwhelmed by the digital world, accepting that their children possess better technical knowledge. But, if we want to keep our children safe online, they need to keep up-to-date with the latest technology'.

Story from: TES

BBC launches Own It website to help under-12s navigate online risks

New site for nine to 12-year-olds is part of corporation's £34m investment in children's programming over three years.

Story from: The Guardian

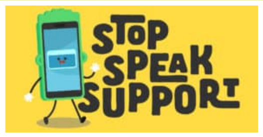
Under-age social media use 'on the rise', says Ofcom

Half of children aged 11 and 12 have a social media profile, despite most platforms' minimum age being 13, a study from regulator Ofcom suggests.

Story from: BBC

For more on any of these stories, visit our school websites where we regularly feature a news roundup of key Online Safety news stories.

Stop, Speak, Support...



...when you see online bullying.

Stop, Speak, Support was created by The Royal Foundation's Cyberbullying Taskforce – a group of industry, charity leaders and young people working together to address cyberbullying.

Visit the campaign website www.stopspeaksupport.com designed for children to learn about the code and how to apply it in real situations.

Pledge to share the code with kids to encourage them to be good digital citizens and make an impact to stop cyberbullying.

10 Tips for staying safe online at Christmas

With a huge increase in sales of devices (around 13 million people receive smartphones for Christmas each year) it is important to ensure that you and your children are safe when playing with new devices and electronic toys.

To help, we've set out a few top tips to help keep your household safe online over the holidays.

1. Learn your way around

Most devices have controls to ensure that kids can't access content you don't want them to. Make sure your "in-app" purchases are disabled to avoid a nightmare surprise in the new year: www.saferinternet.org.uk/advice-centre/parents-and-carers/parents-guide-technology

2. Take care with tablets

Tablets are really popular with younger children, and the market has several which are geared towards child friendly content. When it comes to using them, start slowly, only download games and apps you have checked out carefully (sites such as www.net-aware.org.uk, or www.commonsensemedia.org provide useful advice) and steer them towards age targeted content such as www.bbc.co.uk/iplayer/cbeebies/features/iplayer-kids or YouTube Kids.

3. Careful consideration

If you have older children, and are thinking about getting them a new phone for Christmas, this can pose its own challenges.

The old online safety messages about having your home computer in a communal place become defunct, because phones are literally mobile computers and have the power of most traditional desktop PCs.

4. Agree screen time

Agree a time limit or number of games beforehand, to avoid repeated disagreements around how long they can spend online.

5. Sleep comes first

It is advisable that the phone/tablet stays out of the bedroom to avoid those night time interruptions.

6. Request access

If you're genuinely concerned about them, ask them to allow you access to the phone/tablet.

7. Monitoring vs having a conversation

It is possible to install software onto devices that monitors online activity, alerts you to inappropriate behaviour, and can block access to certain content. This kind of software is becoming increasingly popular, but while this might sound tempting, it does pose a number of issues around your child's right to privacy & could have an impact upon your relationship with them. The best advice we can give is to talk to your child regularly and openly about behaviour and risk, so that they know they can come to you if something goes wrong.

8. Whole home approach

Consider setting parental controls on your WiFi. You can block access to inappropriate or adult content, and set time limits which may help rein in those excessive Minecraft sessions. The UK Safer Internet Centre has advice on this here: www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider.

9. Gaming with caution

Finally a word about games. This year there are so many exciting games and consoles around, there is a good chance you might have one in your house. Whether a DS, Nintendo Switch or PS4, there is something for everyone, and every age.

Consider whether your child is mature enough to join an online community, and whether the games they are playing are appropriate. For more advice on this visit www.pegi.info or www.askaboutgames.com.

10. Tech together

Finally, make sure you enjoy your tech together, it's the perfect time of year!

REPORTING ONLINE SAFETY CONCERNS

Visit your child's school website for advice and support including how to report online safety concerns:

www.heathfld.bham.sch.uk, www.princealbert.bham.sch.uk,
www.hifield.bham.sch.uk

If you have a concern regarding your child's use of the internet at home or in school, please feel free to contact us. Our school websites have loads of advice and support to help you to keep your children safe online and include information on how to report online safety concerns. If you would like to talk to us about a concern, please come into school and ask to speak to one of our Online Safety Leads.