GUIDE TO MOBILE WEB SAFETY

HELPING TO KEEP YOUR KIDS SAFE ON THEIR MOBILE PHONES

WITH PROFESSOR TANYA BYRON

Visit carphonewarehouse.com/mobilewebsafety

Carphone Warehouse

Introduction – Andrew Harrison, CEO, Carphone Warehouse

With more than 2.8 million children now owning a smartphone, including almost a million children under the age of 12, it's clear that parents see the many benefits children gain from having one.

Now, as more phones than ever come with internet access, the risks children are exposed to are ever more prevalent. Here at Carphone Warehouse, we want to make sure that the potential risks are minimised as much as possible.

That is why last year, Carphone Warehouse pledged to support parents and help them understand the risks that can be associated with buying a child their first mobile phone. We conducted research amongst parents to inform an advice booklet, written in partnership with Professor Tanya Byron.

This year, we want to develop our understanding, and what better way to do that than by listening to the kids themselves? For the first time, we've conducted our research amongst children aged 8-15 years old in order to develop our knowledge around their usage, habits and experiences online.

Again, we're working in partnership with Professor Tanya Byron to give you the best advice out there.

On examination of these results and the latest findings from her own work, Professer Tanya Byron will offer practical help that's easy to implement.

We also support the charity Get Connected, which provides free and confidential help for young people. Visit **www.getconnected.org.uk** for more information.

2.8 million children now own a smartphone in the UK

Introduction – Professor Tanya Byron

With the capabilities of mobile phones increasing, children are using incredibly sophisticated smartphones as part of their daily mobile lives. What this means is that they have the ability to do much more in terms of communicating, socialising, playing, creating and publishing content as well as many other activities previously confined to a home PC or laptop.

However, while for our developing digital citizens this is brilliant in terms of digital opportunities, it also means that as parents we need to focus more carefully on preparing our children to use these sophisticated smartphones safely and responsibly, because with greater digital opportunities come greater digital risks.

This booklet is an update from the original version published by Carphone Warehouse in 2010. Why an update? Well, given the speed of technological innovation, our advice needs to keep up with the children and young people and the exciting array of new, increasingly sophisticated kit that they are using.

Given the amazing opportunities technology offers our children in terms of learning, communication, socialising and play, the advice in this booklet is not to alarm but to empower. As the next generation of mobiles become widely available, we need to make sure we enable our next generation to use them positively and productively.

SETTING THE SCENE AND RISKS

A smartphone is a mobile phone with built-in applications and internet access. These devices can provide: text messaging; email; web browsing; digital voice service; still and video cameras; MP3 player; video viewing and video calling. They can run numerous applications and so are, in effect, mini mobile computers that enable fast web access and surfing, social networking, the ability to create and publish content, gaming and downloading apps.

In the past three years, the number of children accessing social networking sites on their mobile phones has more than doubled from 15% to 36%

Gaming is the most popular online activity amongst 8-15 year olds

Because smartphones are hand held mini computers they have a huge range of functions which make them a lot of fun to use and very difficult to put down. Given their speed of access to the internet and increased functionality, every kind of content, appropriate for all ages, can be accessed at any time.

However this can lead to:

- ACCESSING INAPPROPRIATE CONTENT
- THREAT TO PRIVACY
- CYBERBULLYING
- STRANGER DANGER
- EXCESSIVE USE
- TECHNOLOGICAL & ECONOMIC RISKS/FRAUD

This booklet will explore each of these issues in more detail and identify ways to minimise the risks of each

SMART TIPS SMART PARENTS

Last year, we introduced parents to the idea of staying smart through the 'Talk-Act-Engage approach' and, despite the advances in technology, these basic principles remain. By supporting, teaching and empowering your child, you can help them stay safe online without needing a sophisticated knowledge of the technology.

90% of children had their mobile phone bought for them by an adult

Talk

- Speak to your child and take an interest in their online lives
- Introduce them to the idea of 'netiquette' – treating others as they wish to be treated
- Discuss the risks outlined throughout this booklet and empower your child to manage them
- Reassure your child that they can talk to you about their experiences online without fear of being told off

Act

- Set network level filters in place to restrict access to over-18 content
- Be aware that Wi-Fi enabled mobile can get around these filters
- Discuss privacy settings on social networking sites
- Say no to social networking profiles if your child is too young (the lowest age limit for most is 13)

Engage

- Have a go online yourself – try social networking, blogging etc to help you develop your understanding
- Work with your child's school to understand their policies
- Look at sites together – especially user generated content – and set rules about what they can look at
- Understand and respect their privacy, particularly for older children/teens. Once they've demonstrated responsibility, take a step back and engage with their online/mobile behavior only when necessary

87% of children do not have parental restrictions on their smartphones

ACCESSING INAPPROPRIATE CONTENT

With smartphones offering faster connectivity and easier navigation, children and young people may access inappropriate content either accidentally or on purpose. Indeed, our research found that 21% of the children reported having accessed websites featuring unsuitable content via their mobile phone. This can cause distress or lead to the viewing of material that is inappropriate for their age and stage of development.

21% of children reported having accessed websites featuring unsuitable content via their mobile phone

Tips:

1. Develop your kids' media literacy – help them think about responsible content choices, learn how to filter, feel able to discuss 'embarrassing' topics with you
2. Understand that kids are curious about sex and also that peer pressure may influence their decision making. Help them think about their own values and respect for themselves and the opposite gender
3. For younger children, consider buying a phone without web browsing ability or call the network to switch the phone's data function off
4. Investigate the free content filtering features available from some networks before choosing a contract. Our research showed that only 13% of children had parental restrictions set on their mobile phone, compared to 44% of children who had them on their home computer/laptop – despite the devices having the same capabilities
5. However, do be aware that most free content filtering features available from the ISPs do not work over Wi-Fi or on smartphones
6. There are parental control apps available – both on app stores and through some service provides that offer a variety of features including blocking access to the internet via Wi-Fi, Bluetooth etc. Examples of these include Safe Browser and the Parental Control App

THREAT TO PRIVACY

With bigger data storage capacity and state of the art cameras, smartphones make the creating, sending and publishing of photos and videos fast, easy and fun.

However such content can threaten privacy if, for example, images of your child were being posted online without their consent or your child was recording and sending images of others without their consent.

Tips:

1. Think before you post. Discuss the risks of sharing information with friends or others – not only in terms of reputation but also in terms of giving others access to personal information that could be used against you
2. Ensure children are aware that content published to the web is forever – although content can be deleted it is still web archived and can often still be found. Make children aware of the 'digital footprint' they are creating of themselves every time they upload something online and make them think how this could be used against them in the future (e.g: by employers or academic institutions)
3. Treat others as you wish to be treated. Encourage children to never post images of others without their permission
4. Make sure there is no personal and/or sensitive data being stored on the phone as it could fall into the wrong hands by being either lost or stolen
5. Google yourself every now and again. It will show kids what is already online about them and what others can see. You may be able to make changes if you don't like what you see by submitting your request via Google
6. Keep communication connections like Bluetooth, Wi-Fi, 3G and GPRS deactivated if they are not being used. Bluetooth, for example, can be hidden and access locked by a password on most handsets. If strangers send invitations to 'connect', encourage children to just ignore in order to avoid unwanted content transfers
7. GPRS tracks the location of the handset. Make sure your kids don't have an open GPRS so everyone – even strangers – know where they are in the world

Over 60% of 15 year olds have accessed a social networking site from their smartphone

CYBERBULLYING

Bullying online – cyberbullying – occurs because just as in the 'real' offline world, there are nasty people in the online world. In addition, many children and young people have not been helped to understand the differences between face-to-face communication and digital communication: it is so much easier to send nasty communications digitally than to do so when you are in front of someone.

Our research shows it's a very real problem – 18% of 15 year olds admitted to bullying, or being victim to bullying, by calls or messages on their mobile phones. Indeed, the smartphone can be a quick and uncensored means of bullying, harassment and intimidation.

6% of 15 year olds admitted to bullying and 12% said that they had been a victim of bullying by calls or messages on their mobile phones

Tips:

1. Introduce and explain the concept of 'netiquette' – treating others online the way they wish to be treated
2. If a child is the target of cyberbullies, encourage them to ignore the communications and never respond or retaliate, as this can just make things worse
3. There are various functions available on social networking sites and messaging apps that can block users, preventing them from sending nasty messages. Try to save and print out any bullying messages, posts, pictures or videos that are received or seen; make a note of the dates and times of bullying messages, along with any details you have about the sender's ID
4. If cyberbullying is repeated, change user ID, nickname or social networking profile
5. Ensure they understand the concept of protecting their privacy and keeping personal information private. Never let anyone have access to their passwords and check the privacy settings on their accounts
6. Report any cyberbullying to the CyberMentors, whether it's targeted at you or not and receive confidential support and advice. (http://cybermentors.org.uk)
7. Get Connected is a charity that can help you find help for your child if you don't know where to turn to. Visit **www.getconnected.org.uk**

STRANGER DANGER

Online, there are lots of ways that strangers can deceive children in order to get to know them.

'Grooming' is a term that refers to ways in which an adult will try and seduce a child. First by becoming one of their 'trusted' friends online, offering a listening ear and then by getting them to agree to sexual activities or blackmailing them via a compromising image they may have already sent. The aim for that adult is to meet that child in order to engage in sexual activity with them. This can occur by receiving calls/texts/pornographic content from known or unknown adults.

'Sexting' may also become an issue – though not necessarily just with strangers. The term refers to the creating, sending and receiving of sexual photos or videos. This may happen naively in the context of a 'relationship' but such content can be used against the sender e.g: via cyberbullying; grooming; blackmail (called sextortion).

Tips:

1. Encourage your children to only add or accept invitations from friends when using smartphone services and applications – e.g: messaging and social networking sites
2. Highlight the risks of speaking to or messaging strangers online through their smartphones
3. Ensure they understand they should NEVER meet anyone offline (in the real world) that they have only ever met online – they may not be who they say they are
4. Explain that by possessing or distributing sexual or indecent images of another young person (under the age of 18) they are technically in possession of an indecent image of a child which is an illegal offence
5. Such images could be accessed by sex offenders on the web who could then use the image, circulate it or attempt to blackmail the subject
6. For support and advice see **www.thinkuknow.co.uk** or visit **http://ceop.police.uk** to report the receipt of indecent images via the CEOP REPORT button

38% of 10 year olds have reported receiving unwanted calls or messages on their mobile phone

EXCESSIVE USE

While smartphones have many features which can provide endless entertainment, some kids and young people can start to show signs of dependence on their phone. It may never be out of their hand and/or in use all time.

39% of children keep their mobile phone switched on all the time

In turn this can lead to:

- Phone use getting in the way of offline life – e.g: socialising, doing homework or sleeping
- Anxiety if the phone is not nearby
- Huge phone bills

Tips:

1. Set up a daily or weekly limit – both for time spent on the phone and monthly cost. Some service providers such as T-Mobile offer capped contracts
2. If there is an unexpected increase in a phone bill, use features and/or applications which can warn you of increased use, or lock features of the device like the internet. Apps available include Norton Mobile Utilities and SystemPanel App/Task Manager
3. Pay As You Go phones can limit use because once the credit has been spent it can't be used until it is topped up
4. Some service providers and handsets offer parental controls that have settings to block texts and calls
5. Ensure there are parts of the day when the phone is not used – e.g: mealtimes, homework time or bedtime
6. Enforce strict rules and confiscate the phone if these are broken

TECHNOLOGICAL AND ECONOMIC RISKS FRAUD

Because smartphones have an increased capacity to store personal and confidential information there is an increased risk of viruses and spam. In addition, downloads and file sharing can all lead to kids revealing personal details without them realising. Downloading applications (apps) can also lead to personal details being gathered and revealed to third parties.

Only 1 in 5 children have security software installed which stops viruses infecting their mobile phone

Tips:

1. Ensure the same safety measures are taken with the smartphone as those used with the home PC. Our research shows that 46% of parents are unaware of the necessary controls to protect children's mobiles, which is leaving lots of smartphones exposed. Precautions you can take include installing antivirus software - which is included in Geek Squad's Max Mobile policy (**www.geeksquad.co.uk**) - using a password or PIN and automatically locking out the device after a period of inactivity

46% of parents are unaware of the necessary controls to protect children's mobiles

1. Discuss and supervise the downloading of apps or files as they may contain harmful viruses. Only download official apps or those coming from trusted sources
2. Discuss that some app stores/individual apps may be able to access a range of data on the phone including: contacts, location, unique IDs and that this information may be shared with other companies
3. Some apps have been created by hackers that can infect the device with viruses – this will show if the device starts sending emails/texts not written by the owner. If you think this has happened, call the device manufacturer or install security apps
4. Investigate options for your phone and/or network. For example, the app Android Parental Control (free) restricts access to apps and AppNotifier (free) will let you know when your child loads apps onto the phone

SECURITY CONTROLS

O2

Our free Parental Control service limits the websites children can use on their mobiles. It only lets them use sites that have been classified as suitable and interesting for children under 12.

To turn Parental Control on **call 61818** from your child's mobile.
Or visit o2.co.uk/parentalcontrol.

Vodafone

If your child has a Vodafone mobile, you can request Vodafone Content Control. Or, it might already be set as default to restrict access to content that has been rated as only suitable for over 18s, such as gambling and erotic content.

Visit: http://www.parents.vodafone.com/introduction

Talkmobile

Access to adult content is restricted on all Talkmobile Pay As You Go, World, Pay Monthly, SIMple and Control plans.

Visit: www.talkmobile.co.uk

3

All Three mobiles have a filter to automatically block access to websites with 18+ content. Customers can enable over 18+ content by contacting Three's call centre.

Visit: http://www.three.co.uk/Support/Internet_and_Apps

Orange

The 'Safeguard' service blocks content unsuitable for under 18s and it is pre-installed on PAYG accounts. Activate it on Pay Monthly contracts by calling 07973 100150.

Visit: www.orange.co.uk/safety

T-Mobile

T-Mobile's Content Lock blocks content that is inappropriate for under 18s. It is on by default for both prepay and contract customers on all devices including dongles and BlackBerrys. There are three settings: Strict; Moderate and Off. The default setting is Moderate which blocks adult content but allows social networking and chat sites. Text MODERATE to 879 or text STRICT to 879.

Visit: www.t-mobile.co.uk/adviceforparents

Virgin Mobile

By default the network blocks 18+ content and customers can turn off Parental Controls by confirming that they are over the age of 18 either through 'Your Account' on their website, or by calling 0845 6000 789.

Visit: www.virginmedia.com

Notes

Notes

FIND OUT MORE

To find out more about how to keep your child safe on their mobile phone, the following sites may be:

www.kidsmart.org.uk

www.thinkuknow.co.uk

www.ceop.police.uk

www.iwf.org.uk

www.cybermentors.org.uk

www.getsafeonline.org.uk

www.beatbullying.org

www.childline.org.uk

Visit **carphonewarehouse.com/mobilewebsafety**

Carphone Warehouse

ZZVMWEBSAFETYLEAF12 (930046647)