e-Safety for Parents

Helenswood Academy

Published June 2014

Contents

Introduction

Freedom on the World Wide Web is the same as freedom in the outside world. As a child, there are places they shouldn’t go, there are times when they shouldn’t be online and there are people they shouldn’t talk to.

This booklet will assist you to better understand the Web, the way children use it, the dangers involved and, as a parent, what you can do about it.

The Web

As the Internet grows, the Web grows with it. “What’s the difference?” you ask.

- The Internet is every computer, every mobile phone, every tablet, in fact, everything that connects to the Internet, IS the Internet.

- The Web is what you see and use: sites like eBay, Facebook and Tesco form part of the Web. Every email you send uses the Web.

As more people in the world connect to the Internet, the Web gets bigger and bigger which means both the good and the bad get bigger too.

Children online

Most children, if not all, use the Web to communicate with their friends. While technology can’t be stopped and social interaction between children moves online we as parents need to consider how we protect our children exactly the same way as we protect them when they are outside in the real world.

There are three areas we feel need parental attention:

1. Friends
2. Information
3. Ownership

1) ‘Friends’ of your child

According to a recent survey the average 12-15 year old has 272 social network friends. That’s a lot! Being in a school certainly helps but it’s extremely unlikely that any child has that many friends.

Most social networks require friends to be ‘accepted’ which offers some protection but some can attract ‘followers’ which allow random people to follow your child’s activities.

Children often like the attention a ‘friend’ can give so friends are accepted without a second thought. The problem is an online friend is just a made up profile which represents a person and there is no guarantee that representation is genuine.

Is that person real? Has your child met them? Does your child know them?

2) ‘Information’ about your child

Most children post too much information. Compound this with a complete misunderstanding of the privacy settings and on the Web you have all you need to know about your child’s likes, dislikes, their current whereabouts, their school, their friends and much, much more.

A recent trend with apps such as Snapchat is to send inappropriate photos. This is in the belief that photos sent by Snapchat are safe because they are automatically deleted but anybody can take a screenshot and save the image. Once saved, that inappropriate image is permanently on someone’s phone and ready to share with the world.

Information on the Web is public or potentially public, even if it’s private.

3) ‘Ownership’ of your child’s technology

Phones, Wi-Fi Internet, text messages, data contracts; they all add up. Keeping a phone for a child with all these services can be expensive.

Given the dangers of privacy on the web and the freedom children have with their phones, it’s time to take back ownership. Ownership of their time online, the information they post and the technology they use.

As a school we occasionally deal with children’s use of the Web and we see mid-week conversations between students occur at 1am, 2am, sometimes later. If a child is up at that time of night then it’s likely they’ll be too tired to learn the next day at school.

What are children doing?

Everything!

- Children are sharing pictures and messages on social sites such as Facebook, Twitter, Snapchat, Ask.fm and KiK.
- They’re learning by watching videos, reading articles and sharing knowledge (*we like this*).
- Online gaming is hugely popular whether it’s a PlayStation or an iPad.
- Downloading films and music whether paid for or illegal using torrent software.

The dangers

There are many but the biggest dangers are bullying, strangers and reputation.

Bullying
Bullying in all its forms is destructive and children need protection from it. When a child has Internet freedom, they are then free to both give out and receive bullying.

Strangers
With too much personal information on the Web, children become vulnerable to strangers, people who see them but don't know them such as shopkeepers, neighbours or even ex-boyfriends / ex-girlfriends.

Reputation
Swearing, inappropriate images and general bad attitude don't go well with schools, colleges or employers.

Apps

You may be familiar with names like Facebook, Twitter, Google and Yahoo. They provide a wide range of Web services, many for free. They also provide a range of services called apps which live on mobile phones and tablets to help make it easier to use their services.

Apps are also developed by independent companies and come in all shapes and sizes such as shops, chat, image sharing, socialising, games, books and music. There are literally millions of apps available and many are free to download.

We'll list the most popular apps we know children use and explain what they do, how children use them and any associated risks involved.

Facebook

The world’s biggest social network is very popular with children and rightly so. It’s an easy to use and powerful way of sharing your life with your friends through images and messages, likes, groups and interests.

Facebook has very good privacy control but **you need to be sure it’s configured correctly**. Most children care less about their settings and more about their friends. In a race to gather as many friends as possible to be seen to be popular, nearly everyone is accepted as a friend. When you consider that most Facebook profiles contain family, real friends, photos, events, locations and more, **it’s very important that every single Facebook friend is someone your child knows and trusts**.

Twitter

Children use Twitter to send and read short text messages. Twitter also attracts ‘followers’. By default, Twitter is a public service so anyone can send, read and follow anyone. **This means that whatever your child posts is public**.

The danger here is Twitter is often used like a private messaging service and the conversation can reflect this. When inappropriate messages and images are placed on Twitter, other followers can copy them and they are saved on the Web forever. Followers can be anyone in the world so it’s not a secure service for any child.

Children need to be sure that they ‘think before they post’ and if they expect privacy, they need to set their account to private.

YouTube

The biggest video website in the world is also one of the best learning resources in the world. We love YouTube and so do children. **With ‘safe mode’ on most inappropriate content is removed** so it's a good and fairly safe place to spend some time but unfortunately ‘fairly safe’ and ‘some time’ are the problems.

The safety system in YouTube will never be 100% safe for younger viewers so parental supervision is recommended.

Also, due to the sheer amount of videos about every conceivable subject, children can view YouTube endlessly but the amount of time spent can quickly become unhealthy. **Just like you would limit the TV, limit YouTube too. Lights out after 9pm.**

WhatsApp

A Web-based instant messaging service where children can chat with their friends for free. WhatsApp uses their mobile phone number to manage contacts which makes it very easy to connect to others.

When WhatsApp is installed the privacy is set to public which means anyone can find and send a message to your child.

It’s important for all WhatsApp users to make sure that in Settings / Privacy, all options are set to My Contacts.

This will help further protect your child from being found and messaged.

Kik

Another very popular instant messaging service that gives children the opportunity to share text messages, sketches, voice messages and other content.

Kik is open to anyone and **children can receive messages from anyone unless they select the setting ‘ignore new people’**. This will mean only those people your child has contacted can send a message back to them.

It’s also best to let Kik find new Kik users than to publish the username on the Web somewhere as this can attract unwanted messages.

Instagram

A massive photo-sharing website where children can socialise around those images by passing comments, tagging and liking. It’s hugely popular and a wonderful place to spend time keeping up with friends but it’s also a public service and this means inappropriate content and strangers looking at personal photos.

Due to the public nature of Instagram **children should think before they post** and **parents should supervise their child’s use of this service**.

Snapchat

A current favourite with children due to the quick way they can send and receive photos with their friends.

Snapchat photos, known as ‘snaps’ are sent from one phone to another and then when they are viewed, they are automatically deleted forever. This makes children feel safe so they can push their luck by sending inappropriate pictures.

Unfortunately, Snapchat is not safe and pictures can be saved.

When using Snapchat **your child is also vulnerable to strangers posting inappropriate photos** because the default security setting is to receive snaps from <u>anyone</u>. This setting needs to be changed to <u>friends only</u>.

Ask.fm

A popular and free question and answer service that children use to get attention from their friends. **Ask.fm has a poor reputation for bullying and it’s a service we seriously discourage children from using**.

When your child uses Ask.fm, they are vulnerable to everybody in the world who has a connection to the Internet but the single biggest concern is that anyone can ask your child a question with total anonymity. This presents a huge danger to your child. **It’s one of the most abusive online services we’ve seen and the kind of questions or messages sent to children are very disturbing**.

If your child has an Ask.fm account, please do monitor this very carefully.

How children get around restrictions

So, you’ve taken control of your child’s use of the Web, restricted your Internet connection or their phone, tablet or computer is switched off before bed. Children are incredibly ingenious and the Web is an overwhelmingly attractive place to be.

Below is a list of the common ways children beat the rules:

- **Hiding equipment** – “I can’t find my phone right now so I can’t be on the Web, can I?” is the most popular one.

- **Sharing phones** – second-hand phones have little value these days so children often pass around phones to each other with credit on them so there’s access to the Web.

- **Hot-spotting** – Most modern phones have the ability to pretend to be a Wi-Fi Internet router. One child goes to school with their hot-spot turned on and every other student can connect to that phone and receive free Web access.

- **Neighbours** – Just because you've set parental controls and limited access, doesn't mean your neighbour has too. Did your child pop round to help a neighbour with their computer? It's likely they have their Wi-Fi password. Remember, Wi-Fi signals go through floors and walls!

- **Resetting the router** – Most routers come with a tiny reset button. Once reset, enter the default username and password and you've got access to everything, including filters.

- **Proxies** – A proxy is a Web service which fools another Web service. It lets them think the user is someone else. It’s used to gain access to restricted material, usually age-restricted or content in other countries.

- **PlayStation / Xbox / Wii / TV** – Most game consoles, even modern ‘smart’ TV’s have Web access which means your child can access their favourite sites like Facebook, Twitter and YouTube on these devices too.

What you can do as parents

There are two aspects to consider, working with the technology and working with your child.

Technology is the difficult bit because there are so many elements involved but let’s start at the beginning which is your Internet Service Provider (ISP) and their parental controls.

Parental controls

The best way to address the safety of the Web is to control it using your Internet Service Provider (ISP). Companies like BT, Sky, Virgin, TalkTalk and PlusNet are just a few of the many services who offer parental controls. This is an effective way of screening content before it’s viewed.

Because this is usually your single point of contact with the Internet, anything else connected such as smart TV’s, game consoles, tablets and laptops will all be screened too making it an effective step for protecting your child.

For more information about setting up parental controls for your ISP, **please go to page 29**.

Games consoles

Xbox, PlayStation and Wii all have their own safety settings to help restrict what content your child has access to. These games consoles are often overlooked in terms of Web access but many let you watch films and television programmes too.

Game consoles are also socially interactive. This lets your child make friends, message, chat and video other players from around the world.

Each console has its own safety controls so you'll need to visit their respective websites to know how to set them up.

More information is available on page 29.

Mobile networks

Most pay-as-you-go (PAYG) or contract services offer telephone calls, text messaging and the all-important data. It’s this data that children need to connect to their favourite social networks or apps.

Each network such as O2, Orange, EE, Vodaphone or Tesco Mobile have a range of tools to block or filter inappropriate content. These may block your child from accessing certain websites on their phones or tablets but may not restrict access to certain apps. You’ll need to verify this with your network provider.

More information is available on page 29.

Operating systems

Whether you or your child is a Windows or an Apple user, these computer operating systems have their own set of controls to assist you protecting your child from running undesirable programs, using their computers at certain times of day and much, much more.

There’s too much information on this subject for this booklet so **please visit the resources section on page 29 for more information**.

Resources

Internet Matters is an independent, not-for-profit organisation to help parents keep their children safe online.

Visit www.internetmatters.org for more information about:

- setting parental controls
- securing devices like the Xbox
- managing data access on phones
- advice about cyber-bullying
- more tips and tricks

As a parent, if you have a specific question you'd like to ask you can contact Helenswood Academy on (01424) 753040 and ask for eSafety advice from the IT SUPPORT team.

Parent checklist

Action	Done
Setup parental controls for your broadband	
Setup parental controls for your games consoles	
Setup parental controls for your mobile networks	
Setup parental controls for your operating systems	
List your child's apps and social networks	
Check followers and friends are appropriate	
Check privacy is set to private or friends only	
Check images and messages are appropriate	
Limit the amount of time your child spends online	
Talk to your child about any concerns they may have	
Talk to the school about any concerns you may have	