

WHAT IS E-SAFETY?

E-Safety (Electronic Safety) simply means protecting all users of the Internet, both young and old, and providing guidance to allow them to protect themselves when using technology such as the World Wide Web and mobile phones.

Very often when people talk about E-Safety they are referring to the various dangers that can be encountered online, especially on social networking sites such as Facebook, Twitter, etc.

What are the main risks at this time?

The fundamental risks can be broken down into three primary areas:

1. Inappropriate contact from people on the Internet.
2. Inappropriate content found or displayed on the Internet.
3. Excessive commercialism by organizations targeting unwary users.

Perhaps the biggest danger children are facing at the moment has been brought about by users not protecting themselves adequately on social networking sites. A recent (2014) survey found that 60% of Key Stage 3 (equivalent to classes six to eight at Michael Hall) pupils were not protecting their personal information (photos, contact details, etc.) on Facebook. This means that anyone who searches for the pupils' Facebook profile can view this information.

What are some basic precautions that I can take right now to help protect myself and others online?

- Check that your family are using the security settings on social networking websites in order to set each section of their profile page to 'private' so it can only be viewed by their friends. See the list of sites further down this page.
- Ensure that they are only friends with people who they know in real life.
- Make sure that secure personal details such as mobile phone numbers and contact email addresses are not displayed.
- Consider using a cloud based filtering service such as OpenDNS (see the section on OpenDNS below).

OpenDNS

Without getting too technical, DNS (the Domain Name System) is what's used to turn text addresses that humans understand (like www.bbc.co.uk) into the system of

numbers (IP Addresses) that the Internet works on (like 212.58.244.27). This has a convenient by-product in that if we know what the "bad" websites are from the IP Addresses in the global and public DNS register, we can filter and block them before they reach the end user's computer.

An American company, OpenDNS has taken this idea and made a business of supplying web filtering to corporations and large organisations. They provide the same service free of charge to personal users. Click here for the OpenDNS page on Parental Controls. To use the service you'll need to create an account (free) with OpenDNS which you can do by clicking here and a moment's work with a search engine will give you any number of tutorials and explanations of the system. Click here for a good one to start with and here for the official page on setting up devices.

What about our mobile telephones?

Modern telephones are really just handheld computers and every precaution that we take with a desktop or laptop computer applies just as much to a telephone or indeed any other connected device (Smart TV, Games console, etc.). OFCOM provide an excellent page with up to date links to the various mobile network providers. You can find it by clicking here.

A note on relying on filtering software

There are a number of software applications available via a quick Google search (click here) but no amount of technology can ever replace observation, consideration and education on the part of both children and parents. We must be aware and knowledgeable about the Internet, its good and bad points, its strengths and weaknesses, and its up to us as guardians of these children to make the effort to understand. If we don't understand a technology or application we must all make time to learn. Open accounts in the popular social networking platforms (see the list below) and play with them, look at and understand the security settings, read what other people are saying and, most importantly, talk to other parents and talk to your children.

A list of (currently (not exhaustive)) popular social networking platforms and their security/privacy pages:

- Facebook (Security page)
- Twitter (Security page)
- Bebo (Acceptable use page)
- Pinterest (Account Settings page)
- Snapchat (Security page and Safety Centre)
- Tumblr (Settings information page)
- Instagram (Privacy information page)
- Flickr (Privacy policy and help)
- Vine (Privacy policy and How To)
- Ask.FM (Security page)

Talking about the issues

As you'll know, if you tell your child never to do something most children will ask themselves "why not?", then just try to find out for themselves. Discussing the potential dangers with your children therefore needs care and sensitivity and involves helping them to see for themselves how they might get into difficulty. Most children will respond more positively if you encourage them to be switched on or cool on the Internet rather than giving them a list of "do's and don'ts" Childnet provide a lot of useful and accessible information, including how to discuss these issues. You can find a useful starter page by clicking here.

I'd like more in-depth information. Where should I start?

The question of e-safety and its application is a moving target and as such it's a better idea to understand the overarching concepts rather than trying to get to grips with every eventuality or collection of technologies. When one is aware of the benefits or possible pitfalls surrounding any connected device or online situation it makes it much easier to define and understand new situations as they arise.

A useful starting place for this is the CEOP (Child Exploitation and Online Protection Centre) webpage and its accompanying media portal, Thinkuknow.

- www.ceop.police.uk
- www.thinkuknow.co.uk

You might also find some important information in this online booklet:

https://ableprod.blob.core.windows.net/apps/zm/pdfs/live_streaming_ebooklet.pdf

Updated August 2021