English Schools UK Breckland

E-SAFETY GUIDANCE FOR PARENTS/CARERS

Technology is expanding and being used in many different and exciting ways. New technology is being released all the time letting us access information online and communicate with people around the world.

How Can I Be Safe?

There are many steps that you need to take to be safe online, this includes everything from virus protection to checking you have an up-to-date internet browser.

Recommendations

Anti-virus: Check you have anti-virus protection, school staff are entitled to use the school anti-virus software. Students and Parents remember there are many free anti-virus packages available. Make sure your anti-virus is up-to-date; most anti-virus programs integrate into Windows and notify you if it needs updating. If you are using a laptop offline remember to connect it to the internet to update the anti-virus definition regularly.

Operating Systems: It is always best practice to ensure that your operating system is up-to-date. Operating system manufactures release updates to patch security holes found since the release of their OS. To turn on automatic updates in Windows XP do the following; Start > Control Panel > Security Centre > Turn on Auto Updates.

Internet Browsers: A modern browser is integral to your safety online; features such as Phishing Protection help you to avoid giving out personal information to sites posing as legitimate sites. Peer

2 Peer and Warez: are notoriously dangerous and a high risk area for infecting you with viruses and spyware. Whilst they do offer many legal uses, P2P programs are generally used to share illegally ripped videos and music.

Email: Many anti-virus programs come with an included plug-in for scanning emails. Additionally online email providers such as Hotmail, Gmail and other web based email systems, such as ones provided by your ISP offer online email attachment scanning. However it is always best practice not to open attachments in emails sent by an unknown address

So how do I know where is safe?

There is no definitive list of websites which are safe and not safe due to the sheer size of the internet. Although some modern browsers link back to a database online and warn you if you are attempting to visit a site known to be unsafe, to help you keep safe we have compiled some information to help you:

Golden rules for family internet usage

1. Keep personal information confidential. For example do not give out your name, date of birth, phone number or any banking/credit card information.

2. Discuss internet usage with your son/daughter and get to know the services and websites they use.

3. Do not believe everything you read or see online, there are numerous bogus websites and email services trying to access your personal information.

4. Encourage your son/daughter to tell you anything they find that is suggestive, obscene, threatening or makes them feel uncomfortable.

5. Do not immediately blame your son/daughter if they receive or access something obscene – this may have been done accidentally.

6. Only use one account for online transactions.

7. Be careful when using online shopping facilities, for instance after each purchase print off your order with the company's confirmation number, date and total amount spent.

8. People in chat rooms, instant messaging services, and even facebook 'friends' may not be who they appear to be.

Websites

The quickest and easiest way to navigate the internet is by knowing the address of the site you wish to visit, but this can be a very impractical method of navigating the World Wide Web. Many search engines offer a 'family friendly' search by default, although you should not rely on this as your only solution.

Many websites contain age restriction stating if a site is for persons of a certain age, although the checks done to gain access just ask for a date of birth or a simple 'are you 18, YES/NO'. Programs such as 'NetNanny' and 'Cyberpatrol' offer a live protection against site content, but this kind of software has proved to genuine sites and still allow illegitimate sites.

Downloads

Only download files from trusted sites, if you are suspicious of the legitimacy of a website don't download any files from it.

Internet Chat Rooms

Internet chat rooms are by no means a bad thing, like the rest of the web they offer many valuable resources, and contain a great deal of educational value but beware there are certain chat sites that will prey on the young and vulnerable.

IM (Instant Messaging)

Whilst instant messaging applications can be an important part of collaborative work there are also many risks that this software can offer. Parents remember you have no way of knowing who your son/daughter is talking to, and more importantly, sometimes nor do they. They can be exposed to foul language or inappropriate sexual content. It is important to remember that some young people have actually being arrested for producing and sharing pictures of themselves, with the person they

sent it to also being arrested for being in possession of child pornography. It is important to monitor use of instant messaging use via chat logs and checking 'received files' folders (contained in My Documents\My Received Files' with chat history also being contained in a sub folder here – true for MSN Messenger and Windows Live Messenger). Whilst anti-virus programs do scan IM applications they are not fool proof and do rely on being up-to-date.

Important rules of thumb for IM Applications

- If you get added by someone you do not know be cautious about giving away personal information. Not real names (or at the very least no real surname).
- Do not give away where you live, country and county are ok, but never town/city.
- Never accept files being sent from an unknown 'IM Buddy'.

E-Bullying

Bullying is a big concern for parents and can distress many students, so online bullying should not be treated any differently. E-Bullying is particularly harmful as internet/electronic facilities are available 24hrs a day and can reach the victim in his/her home, where people generally feel safe. Unfortunately it is not immediately possible to check the origin of an email, the best advice is:

1. Block the bully - If bullying happens through a personal email account, report it to the sender's email account provider – you can find this after the @ sign. If it is not obvious who the sender is and there is continual bullying using email, then there are tools to trace senders. To find out more about this email tracking, go to one of the search engines (e.g. Google, Yahoo etc) and type in 'email tracking software' – this software can be downloaded. Once you know the identity of the bully get in touch with your internet service provider (ISP) who can then block the sender from your email.

2. Don't retaliate or reply

3. Save the evidence

4. If the email bullying is occurring in school, then this should be dealt with through the school's anti bullying policy.