

KEEPING YOUR CHILD SAFE ON THE INTERNET

Guidance for parents and carers on the safe use of the internet at home

The internet is now a way of life for most of us and increasingly so for our children. They are using it at school and often as part of their homework, and more and more they want to use it at home for their own entertainment. They have at their fingertips an amazing opportunity for constructive learning, communication and fun and we should certainly be encouraging them to use the internet to its full potential but there are also risks associated with it. We are therefore all anxious to ensure that our children learn to use this powerful tool safely. Here are a few practical tips that may help.

What are the risks?

It doesn't take much imagination to work out the potential dangers of children making contact with inappropriate people through chat rooms and of children seeing ghastly images on the screen. Less obvious perhaps are security issues such as people getting hold of the family's personal details (address, bank details etc) or simply of your computer getting a virus which could wipe out data, make the computer temporarily unusable or allow unsuitable material through without warning. So, be aware that risks arise from:

Contacts – use of chat rooms, often leading to email or instant messaging (i.e. real-time email)

Content – accessing of pornography, violence, racism or just inaccurate information

Security – privacy issues, computer function and viruses.

What should you do?

Don't panic!

First: you don't need to be a computer expert – we are all able to help and protect our children, whatever our own level of expertise.

Second: try not to over-react to the dangers as this can lead to children being more secretive about their internet activities.

Third: understand what you have at your disposal to help. These include:

1. SUPERVISION

There is no replacement for on-going parental supervision.

Consider:

- putting the computer in a family room rather than your child's bedroom to prevent secrecy and improve your knowledge of what they are doing
- using a password on the system that only you know so that they cannot log on when you not there
- talking to them regularly about internet use – what the risks are, what they should do if a problem arises, what controls you have put in place and what you consider to be off limits (perhaps for older children think about agreeing an internet contract through which they agree acceptable rules for internet use – where they should not be visiting etc.

2. TECHNICAL HELP

Think about the technical controls available.

- **ISPs** (internet service providers) often offer safety tools so parents should check with them first to see what is available. For instance, it might be possible to obtain special children's web browsers and search engines so telephone your ISP or visit their website to find out the options.

Software It is possible to buy specialist software. Basic security software will protect against viruses and unwelcome intrusions. Child orientated security software packages (ie. Net Nanny, Porn Blocker, Family Net, Norton etc) will also include:

Filters and controls - which block unsuitable content or control access to particular sites

Monitors - which record web addresses visited or which put up a warning before a site is accessed stating that the parent thinks it is not suitable

Time limiters - which limit the amount of time or the time of the day a child can use the internet (for example, when the parent is out at work)

Tools that prevent out-going content - such as personal details.

However, whilst these products and services do offer protection, none of them can be relied upon by parents as a complete solution. No software is 100% effective, children may find a way of avoiding the controls, they may do so by mistake or a virus may still get through and temporarily over-ride the other controls. Therefore the best option for parents is the use of software in addition to careful supervision AND

3. ACTIVE MANAGEMENT OF YOUR COMPUTER

Think about what you can do to keep your computer working well for you and the family

- make sure your security software is kept up to date and functioning properly
- act on any security "up-dates" sent from your operating system provider (eg. Microsoft)
- change any passwords regularly
- routinely check any controls you have in place, for instance to find out what sites the children have visited and perhaps who they are communicating with
- delete spam (ie. email from strangers) and be careful what you open if you do not immediately recognise it and think about anti-spam software where possible
- consider keeping your own data and internet access separate from your child's (for instance, some providers allow several accounts for added convenience and security).

And remember, there is a lot of support you can draw on if you get stuck on the technical stuff – you will probably have access to one or more help lines run by either the people you bought the computer from, the operating system provider (e.g. Microsoft), the software manufacturer or your internet service provider (e.g. Freeserve).

BUT ABOVE ALL, TELL YOUR CHILD TO BE INTERNET SMART!

S – keep personal details **secret**

M – never **meet** anyone you have met on the internet unless parents have consented and are present

A – don't **accept** emails, open attachments or download files from strangers

R – **remember** people may not be who they say they are

T – **tell** someone if you are worried

Some useful addresses

thinkuknow.co.uk childnet.int.org
getnetwise.org safekids.com

CYBERBULLYING – Information and Advice for Parents.

There is increasingly public concern about the amount of cyberbullying that takes place involving children. We feel that this problem is rare in primary schools and is one that has not presented itself as a problem at Honeywell.

However, we do feel that it is important for all parents to be aware of its potential and of the measures we have taken to deal with cyberbullying should it arise at Honeywell.

What is cyberbullying?

Cyberbullying can be defined as *the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.*

Categories of cyberbullying may include:

- Text messaging and email bullying – sending unwelcome or threatening texts/ messages.
- Picture/ video clip bullying via a mobile phone – images sent to embarrass, ‘Happy Slapping’.
- Phone call bullying – silent calls or harassment.
- Chat room and IM [instant messaging] bullying – sending menacing or upsetting responses through a web based chat room.
- Bullying via a website – defamatory comments posted on websites such as BEBO, Facebook or personal websites.

What the school is doing.

At Honeywell we have a clear code of conduct for using the internet at school. Children are not allowed to use chat room facilities at school and any communications made via the school’s computers are monitored. It is unlikely that any form of bullying using school computers will take place.

Children are not encouraged to bring mobile phones to school. However, some parents like their children to have mobile phones so that they can contact them after school. In such cases parents must write a letter to the class teacher and the phones must be handed into the class teacher each morning and collected at the end of the day.

What you could do.

It is essential that you inform the school if you become aware of any form of cyberbullying taking place between your child and another pupil at Honeywell. Be aware of what your child is doing online, classmates may be using a chatroom to communicate, check that your child is using the chat room safely.

Additionally, most software and services on the internet have in-built safety features. For example, IM services such as MSN Messenger have features which allow users to block others on their contact list, and conversations can be saved on most IM services. Social-networking sites such as MySpace and Bebo also have tools available, e.g. young people can keep their profile set to ‘private’ so that only approved friends can see it.

With bullies using text and picture messaging, it is also important to check with your children's internet or mobile-phone provider to find out what protections they can offer, including whether it is possible to change your mobile number.

What advice to give your child re cyberbullying.

- Don't respond to malicious texts or e-mails and save evidence, keep the cyberbully's messages as evidence.
- Report cyberbullying to a trusted adult.
- Don't give out personal details online and keep passwords safe.

The school Anti-bullying Policy states:

If the school becomes aware of a *cyberbullying* issue that happens outside school time, it may choose to intervene and contact the parents of those children involved or affected.

OUR E-SAFETY RULES



We always ask permission before using the Internet.

We only use websites that our teacher has chosen.



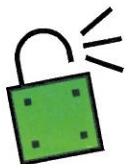
We tell an adult if we see anything we are uncomfortable with.

We immediately close any webpage we are unsure about.



We only e-mail people our teacher has told us to.

We never give out personal information or passwords.



We do not use internet chat rooms.

