Using parental controls

Parental controls are a great tool to help protect your children online. There's plenty of advice available to help you use them and it may not be as difficult as you first thought.

What do parental controls do?

These controls are designed to help parents and carers manage their child's online activities. There are various types, some of which are free but others which can be bought. However, nothing is totally fool proof so they don't replace the need for adults to support and advise children using the internet.

For detailed guidance on all the different types of control, you can use an online tool from Internet Matters - www.internetmatters.org/parental-controls/interactive-guide. This gives you the chance to set up a personalised list of the controls used in your home on all your different devices. There is also advice on how to use all the various controls, with videos and step-by-step instructions.

What can controls be used for?

Controls can either be for a device like a games console, or for a network such as your home broadband.

The way to access device controls can vary according to the manufacturer. They can offer varying types of protection, from filtering out adult content from search results to preventing your child from buying things when playing games. You can generally find instructions on how to set these controls up on the manufacturer's website or use the Internet Matters website for help. These settings will apply whether the device is being used in your home our outside – but it's easy for them to be switched off, so talk to your child about trust and responsibility, making sure they understand the importance of why you have put the settings in place.

Most games consoles come with settings, which can be put in place for either the device itself or the games platform. It's easy to forget that games consoles allow players to connect to the internet and talk to people all over the world so setting controls on devices and the platform itself (such as X Box) is important.

Broadband and network filters generally come free with your service. These can be used to prevent material coming into your home. For example, you could restrict anything with a horror or sexual content being accessible via your home broadband. Instructions for accessing these filters can be found on the service providers' websites – look at the bottom of the page to find the "help" or "security" page.

Online controls

Search engines such as Google, Yahoo and Bing allow users to filter out certain types of search results. This means you can reduce the risk of your child seeing adult content like pornography, or set limits on the time they spend online. Look for the cogwheel "settings" symbol where you will find the options for each provider. You can also encourage your child to use safer search facilities, such as Safe Search Kids from Google.

Social media and other websites

As with search engines, social media and sites like YouTube have privacy and security settings. These can prevent your child from being contacted by strangers or from seeing inappropriate material. It is important to remember that content filters cannot prevent other people from sending offensive or inappropriate messages or comments to your child's account, so controlling who can contact your child is a key step.

Buying controls

It is also possible to buy filter programmes. These can be either solely for filtering purposes, but some virus protection software also offer filtering options.

What next?

Controls are not a single solution to staying safe online; talking to your children and encouraging responsible behaviour is critical. However, controls are a vital first step to helping to protect your child online, and here are seven simple things you can do to use them effectively:

- Set up home broadband parental controls and make use of controls on your home broadband.

- Set controls on your search engine; encourage your child to always use child-friendly search engines, and activate and lock the safe search settings on the browsers and platforms they use.

- Make sure every device is protected. Controls should be installed on every device your child uses, such as their mobile phone, tablet and games consoles (both home and handheld).

- Use privacy settings. Activate the safety measures offered by different sites; social networking sites like Facebook have privacy settings that will help prevent your child seeing unsuitable advertising or sharing too much with other people.

- Block pop-ups. If you're worried about your children accessing inappropriate content though accidentally clicking on adverts in pop-ups, follow the advice from your service provider on how to stop these.

- Find good sites and agree on them as a family. By talking to your child about their interests you can help them find suitable sites to visit and apps to use. Review these sites as they get older.

- Manage their use and access. Children may be very worried that your response to a problem will be to take away their internet access. Whilst this may be an appropriate response in some cases, the threat may be a barrier for a child who needs help. Be aware of this when talking to them about their internet use, and reassure them that they can talk to you or a trusted adult whenever they need to.

This information has been adapted from the Thinkuknow parents and carers website – **www.thinkuknow.co.uk/parents**

Thinkuknow is the education programme from the National Crime Agency CEOP command. The CEOP command works to protect children from sexual abuse and exploitation both online and offline. Thinkuknow offers a range of safety information for children, young people, practitioners and parents/carers

The CEOP Safety Centre offers information and advice for children and young people, parents/carers and professionals on reporting child sexual exploitation and abuse and provides a route to report directly to CEOP – **www.ceop.police.uk/safety-centre.**