GREENWICH safeguardingchildren BOARD

Dear Parent/Carer,

You will be aware the internet hosts many exciting opportunities for education. The online world is a wonderful place for young people to explore, with unprecedented opportunities for learning and creativity, but just like the real world there are risks and dangers they should be aware of and which we should all act to protect them from. The Greenwich Safeguarding Children Board encourages the use of technology as an important part of our children and young people's development but always want them to spend their time online safely. As a parent/carer you can play a significant part in ensuring this.

Just a few simple steps by you can help keep them safe and give young people the awareness to know what to do if they feel uncomfortable about anything they encounter while on the internet.

If you do not wish for your child to be able to access any inappropriate content online, please ensure that their computers, laptops and other devices with internet access are all fitted with parental controls.

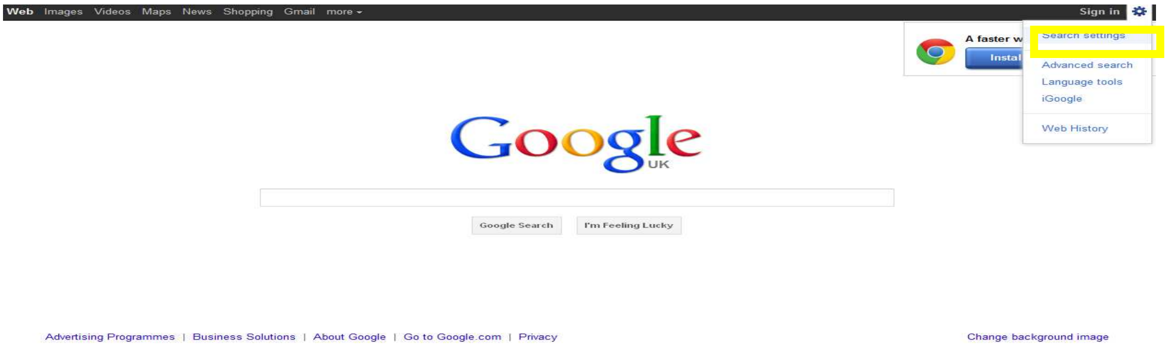
You can find free downloadable versions online or you can contact your internet service provider (such as BT, Talk Talk, Sky) for more information.

As a **minimum**, please set parental controls on your search engines, youtube account and the mobile phone your child uses.

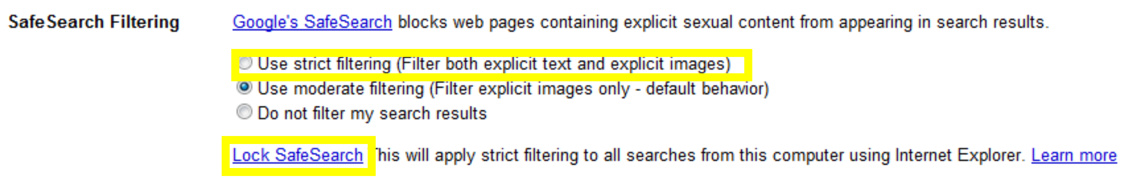
One of the most popular search engines in the world is Google. You can visit Google's informative safety centre for **simple** step by step guides - www.google.com/familysafety/tools

Here are a few options available to you; they truly are simple to set, promise.

Visit the Google home page – www.google.co.uk and click on the 'search setting' tab in the top right hand corner.



Scroll down the page and change the filtering options to suit your family's needs. Make sure you lock the safe search; otherwise these settings can easily be changed without your knowledge.



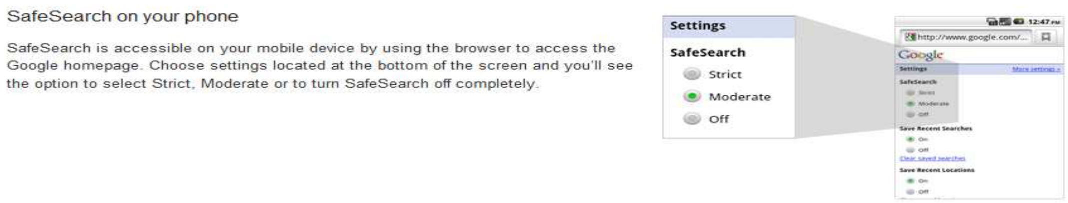
SafeSearch Filtering

Google's SafeSearch blocks web pages containing explicit sexual content from appearing in search results.

○ Use strict filtering (Filter both explicit text and explicit images)
● Use moderate filtering (Filter explicit images only - default behavior)
○ Do not filter my search results

Lock SafeSearch This will apply strict filtering to all searches from this computer using Internet Explorer. Learn more

You can also set this on your child's smart phone;



SafeSearch on your phone

SafeSearch is accessible on your mobile device by using the browser to access the Google homepage. Choose settings located at the bottom of the screen and you'll see the option to select Strict, Moderate or to turn SafeSearch off completely.

Settings

SafeSearch
○ Strict
● Moderate
○ Off

Please be aware that no filter is 100% accurate. CEOP advice that you talk to your child about the sites they use. Why don't you discuss:

- Their favourite online sites
- What they enjoy most, the fun aspects of being online?
- What they think can go wrong?
- How would they react if things got out of control?

Let them know that you understand that situations happen online and that seeing 'adult' material can make them feel uncomfortable. Make sure they know that you are there to help.

Visit The Child Exploitation and Online Protection Centre (CEOP) parents' information website for more information - www.thinkuknow.co.uk/parents

Kind Regards

Amanda Harry

Development Officer

Greenwich Safeguarding Children Board

Keeping your child safe online-A checklist for parents and carers

As a parent you'll probably know how important the internet is to children and young people. They use it to learn, play, socialise and express themselves in all types of creative ways. This may be through sharing photos and videos, blogging,gaming, or even developing their own apps. It is a place of amazing opportunities.

The technology children use in their daily lives can seem daunting. You might worry about the risks they can face online, such as bullying, contact from strangers, as well as the possibility of access to inappropriate or illegal content. To help them stay safe, it's important that you understand how your child uses the internet.

By following this simple checklist, you can start to protect them and decrease the risks they face:

1. I have asked my child to show me sites they use

By doing so, your child is including you in their online life and social activity. Show an interest and take note of the names of their favourite sites. You can then re-visit these when you are alone. Take your time and explore the space, find out how to set the safety features and learn how to report any issues directly to the site.

2. I have asked my child to set their profile settings to private

Social networking sites, such as Facebook, are used by children to share information, photos and just about everything they do! Encourage your child to set their privacy settings to private. They need to think about the information they post online as it could be copied and pasted anywhere, without their permission. If it got into the wrong hands, somebody may wish to use it against them or worst of all try to locate them in the real world.

3. I have asked my child about their online friends

We know that people lie online about who they are and may create fake identities. It is very important children understand this. Whether they are visiting a social network or a gaming site, the safety messages are the same. Children and young people must never give out personal information and only be "friends" with people they know and trust in the real world.

4. I have set appropriate parental controls on my child's computer, mobile and games console

Filters on computers and mobiles can prevent your child from viewing inappropriate and possibly illegal content. You can activate and change levels depending on your child's age and abilities. You can also set time restrictions for using the internet or games. They can be free and easy to install. Call your service provider who will be happy to assist or visit CEOP’s parents' site for further information. Explain to your child why you are setting parental controls when you talk to them about their internet use.

5. My child has agreed to tell me if they are worried about something online – Sometimes children get into situations online where they don’t feel comfortable or see something they don’t want to see. By opening up the communication channels and talking to your child about the internet, their favourite sites and the risks they may encounter, they are more likely to turn to you if they are concerned about something.

6. I know where to get help if I’m concerned about my child

The CEOP Safety Centre provides access to a range of services. If you are concerned that an adult has made inappropriate contact with your child you can report this directly to CEOP. You can also find help if you think your child is being bullied, or if you’ve come across something on the internet which you think may be illegal.

Visit the Safety Centre at www.ceop.police.uk/safety-centre

For further help and guidance on all the information mentioned please visit

www.thinkuknow.co.uk/parents

Protecting your children in a digital world

The digital age has transformed the way we live. Multi-channel TV and the internet means we can now get a wealth of entertainment and information at the touch of a button. But not all of this is going to be suitable for your children. There will be programmes you don’t want them to watch, and web sites which are not suitable for them.

Children often learn about new technology first. Parents will want to help their children get the most from new technology while at the same time helping them to avoid potential pitfalls.

Parental Control functions

With digital TV you can set controls on your TV to restrict specific channels or programmes. In this guide we use Sky as an example but other providers also have their own parental control systems. If a restricted channel is selected in future, your viewing card PIN will be required before you view the channel.

Other digital TV services such as Virgin Media, BT Vision, Tiscali, Top Up TV and Freesat services also have parental controls, as do some Freeview digital boxes and TVs.

If you are unsure how to activate your parental control features or if you want to see whether your system has such a facility check the instructions booklet. You can also phone your service provider, check their website or check with the original retailer.

Protecting children online

When it comes to surfing the net, one of the best ways of protecting children is to educate yourself so that you can educate your children.

- Get to know how your children use the internet. Ask them to show you some of their favourite sites and talk about them. Make them aware that there are things on the internet which may upset them and that they can always talk to you or another trusted adult. Be aware of any changes in the way they use the internet, such as the amount of time they spend online.
- Make sure your children realise they should never give out personal details such as name, address, school and telephone numbers to online friends they do not know in the real world, and tell them never to respond to junk email or open attachments that are from people they dont know.
- Look for local computer or internet classes which will teach you how to use the online services your children are using. Try your local library for information on courses in your area or talk to your childs school about what they are teaching children about staying safe online. Learn how the history feature on your computer can help you monitor the websites that your children are using.
- If you are using a recent edition of Windows or you have a reasonably recent Mac you will find within the operating system or available as a download lots of tools which you can use at no cost. Many of these work with or through the browser. Check with your internet service provider to learn how to block sites you dont want children to see. Its also possible to buy off the shelf filtering software from electrical retailers or online.
- Work with your children to understand how search engines work so that they don’t stumble across unsuitable content and are able to find the information they need quickly and efficiently.
- Help can also be found on websites such as Think You Know and the Internet Watch Foundation. Schools can order free Know IT All CD-ROMs for parents and the Next Generation Learning website has activity cards that you can download to work through with your child.

Useful contact details

- www.thinkyouknow.co.uk
- www.getsafeonline.co.uk
- www.freesatfromsky.co.uk
- www.iwf.org.uk
- www.nextgenerationlearning.org.uk
- www.topuptv.com
- www.sky.com
- www.virginmedia.com
- www.bt.com/vision
- www.freesat.co.uk
- www.tiscali.co.uk
- Know IT All 0845 6022260

From:http://consumers.ofcom.org.uk/2009/10/managing-your-media-protecting-your-children-in-a-digital-world/

Parental Advice on Facebook

Here are some suggested guidelines on how to support your children using Facebook safely:

- The terms and conditions for Facebook state that users need to be 13 years of age. Anyone under that age who has an account is violating the terms and conditions and you can report them at http://on.fb.me/dTSqRP.

- Don’t be afraid to set boundaries for your younger children and explain that, as with other forms of media, there are age restrictions on using certain websites.

- Create a Facebook account yourself and be ‘friends’ with your teenage children. This will enable you to monitor what they post on their wall and who they add as ‘friends’.

- Facebook explicitly states that no person should abuse, harass or bully other people through posts or comments. If you come across any information that breaches this specific rule you can report it to Facebook. Guidelines on how to do this can be found at http://on.fb.me/ePpM93.

- In order to ensure that your teenage children are aware of some of the potential risks on Facebook, make sure that they download the ClickCEOP application, so that they can install the ‘Report Abuse’ application on their Facebook profile. Users can access this at http://apps.facebook.com/clickceop/.

- Ensure that you educate your children about their digital footprints. More colleges, universities and employers are researching candidates for jobs by searching social networking sites. A negative post or unsuitable photograph could come back and haunt your teenage children in later years and prevent them from gaining certain employment.

- Finally, teach your children to send positive posts. Schools and the police are taking seriously negative and libellous comments about educational professionals and it could lead to exclusion or legal action against them.

For further information, visit www.yhgfl.net

Parental controls for mobile phones

Many mobile phones now let you go onto the internet at the touch of a button. This guide will show you how to find information to help keep children safe online when using a mobile phone.

Mobile phones

- All mobile phone providers offer free parental control services which limit the content children can access via the mobile network to items suitable for under 18s. However, they may not always be automatically switched on. Check with your service provider that the parental control settings are switched on, and ask for them to be switched on if they are not. This is particularly important if the phone was used by an adult before.

- Many mobiles can use Bluetooth to send messages, photos and videos between phones. However, this means that other people are able to send unwanted messages which parental controls can't stop. But, you can turn Bluetooth on and off using the mobile handset or you can stop other people being able to access your phone without your permission. Instructions on how to do this should be contained in the handset manual. If you need help, ask your service provider. It is important that you discuss using Bluetooth with your child.

- Young people often take photographs and videos of themselves and each other on their mobile phones but they should be very careful how they then share these images. Embarrassing or inappropriate photos/videos could easily be passed between phones and put online. Once sent or put online, control over the images may be lost and they could end up in the hands of strangers. Photographs or videos may also be used to fuel bullying or harassment. Visit the thinkuknow website for more information and advice on this.

- Chatrooms are popular with children and young people and while mobile providers' own chatrooms aimed at children may be moderated, others might not be. Discuss with your child which sites they are visiting, what's OK to post and what behaviour is acceptable. Visit the Chatdanger website for more information and advice on this.

- If your child has a profile on a social networking site they may access it on their mobile phone. Ensure they know why it is important to allow their personal information only to be shared with people they know in the real world. Most of the larger social networking sites specify a minimum age of 13 for all members. For those sites that are aimed at younger children, parental consent and confirmation of the child's age will usually be required. Check the minimum age requirement for users – ask your child which sites they visit to make sure they're visiting sites appropriate for their age.

Reporting inappropriate material

Our research found that 25 per cent of children and young people say that they're uncertain about what they would do if they came across inappropriate material on their mobile phone.

Parents and carers should encourage their children to tell them about anything they have seen or heard that has made them feel uncomfortable or scared.

Parents and carers should report incidents to their mobile network operator and in instances of sexual contact to the Child Exploitation and Online Protection Centre (CEOP) using their report abuse button.

CEOP REPORT
ceop.police.uk

Some sites also provide a direct link to CEOP, usually through a red button. If you/your child encounter content online that you think might be illegal, there are two things you can do. Firstly, report it to the Internet Watch Foundation (IWF). Again some sites may provide a direct link to the IWF. Secondly, report the content to your mobile network operator.

Further help is available at the following websites:

3: http://www.three.co.uk/Help_Support/Billing_payments/Advice_list

Tesco Mobile: http://www.tesco.com/mobilenetwork/content-mtm.aspx?page=18
O2: http://www.o2.co.uk/support/generalhelp/howdoi/safetycontrolandaccess
Orange: http://www.orange.co.uk/communicate/safety/10948.htm
T-Mobile: http://www.t-mobile.co.uk/help-and-advice/advice-for-parents/inappropriate-content/
Vodafone: http://help.vodafone.co.uk/
Virgin: http://www.virginmobile.com/
IWF: http://www.iwf.org.uk/reporting.htm
CEOP: http://www.ceop.gov.uk/reportabuse/index.asp
ThinkuKnow: http://www.thinkuknow.co.uk/parents/faq/mobiles.aspx
KnowITAll: http://www.childnet-int.org/kia/
Chatdanger: http://www.chatdanger.com/
PhoneBrain: http://www.phonebrain.org.uk

http://consumers.ofcom.org.uk/2009/10/parental-controls-for-mobile-phones/

Mobile location based services

A location based service uses technology to find your mobile's position and provide services related to where you are.

There are two types of location based services.

1. Where a mobile user wants information to be sent to them on their phone e.g. a request for details of the nearest cash machines, the rail or bus station, or for a map or directions to a particular address.

Because the user initiates the service this is called an 'active' service.

2. Where a mobile user is located by another person.

Because the located user is the subject of a location based service initiated by someone else this is called a 'passive' service.

A passive service may help parents know where their children are when they are out and about and have their mobile phone with them.

It is passive services that have raised the most concerns because of the risk that someone is tracked without their knowledge and consent.

How do they work?

Passive mobile location based services operated solely through the mobile phone networks are subject to a strict Code of Practice to prevent misuse.

Passive location based services usually have to be paid for and only a parent or guardian can use them to locate a child under the age of 16. The child must consent before the service can be used.

Text alerts will be sent to the phone as a reminder that the phone is connected to a location based service. The service can be switched off by the parent or the child at any time.

Some of the newer location based services don't use the mobile phone networks at all. Like the original location based services they work through mobile phone handsets, but they obtain the location information in other ways, e.g. by using global positioning satellite (GPS) technology that is increasingly a feature of many mobile phones. The Code of Practice only covers location based services that use location data supplied by mobile operators.

Should I be concerned?

Many of the newer type of location based services are available as downloadable applications and rely upon use of GPS and other location capabilities of the mobile phone.

Some of these services allow the user to share their location information with others, such as friends in their social network or other players in a mobile game. So these services could be a concern to parents, as a child may inadvertently share their location with people they don't really know.

Some downloadable applications are only aimed at adults. However, it may be difficult for the provider of these applications to stop children from getting them.

Tips on using location based services

Here are some tips on using the services and how to help keep your child safe:

• Check the location features of the mobile phone, such as GPS. It may be possible to switch GPS off. If you're unsure how to do that, look in the manual or ask your provider.

• Check what applications your child has on its phone. Usually, these will be stored in an Applications folder, available from the phone's main menu. If you're not sure what they do, open them and see.

• Talk to your children about the risks of posting their location information to a website, particularly if they have people on their friends list who they have only met online. Should anyone approach them to ask if they can locate them, they should decline if they do not properly know them.

• Explain that they should ask you before downloading applications or accepting any service offered over the phone and, if they are not sure, it is always best to check.

• If you think that a mobile location based service is being used inappropriately, tell your mobile operator who may be able to advise or help you.

For more information about location based services and any other services provided by your operator, you can find their contact details here:

• 3: http://www.three.co.uk/Help_Support

• Orange: http://help.orange.co.uk/

• O2: http://service.o2.co.uk/

• T-Mobile: http://support.t-mobile.co.uk/

• Vodafone: http://help.vodafone.co.uk/

From: http://consumers.ofcom.org.uk/2009/10/a-guide-for-parents-and-carers-on-mobile-location-based-services/

Parental controls for games consoles/portable media players

Many games consoles and portable media players now let you go onto the internet at the touch of a button.

This guide will show you how to find information to help keep children safe online when using games consoles and portable media players.

Games consoles

Most modern games consoles let you go online but each console will have different parental controls.

Here are the options offered by some of the more popular games consoles:

- **Microsoft Xbox 360** offers parental controls called Family Settings to help control the types of games and films that children can play or view based on their content ratings. It also provides settings to control the types of interaction carried out on Xbox live. The consoles are automatically set to allow full access so you will need to change the settings to the appropriate rating for your child.

- **Nintendo DS** and **DS Lite** both use PIN (Personal Identification Number) systems so that parents and carers can control downloads, internet access and photo sharing.

- **Nintendo Wii** offers parental controls for game playing and internet use. Game playing settings use age ratings and can be changed to the most appropriate rating for your child. If the Wii is connected to the internet you can restrict use of the internet and sending and receiving of messages.

- Both the **Sony Playstation 3** and **Sony PSP** have parental control settings that restrict the types of games that can be played and downloaded, as well as video content that can be viewed.

Portable Media Players

Portable media players may have in-built parental controls or use Windows Media Player to play video material. The Windows Media Player programme has built-in parental controls, allowing you to set ratings for certain videos.

Archos portable media players have two settings – “Adult (unrestricted access)” when all files are visible and “Child (restricted access)” when files marked as adult content will not be visible. Every time you connect the device to a computer, it will ask for the parental code. A parental code system allows you to create a code and hide any file or folder from view. By default, the device is set to “Adult”.

Reporting inappropriate material

Our research found that 22 per cent of children and young people say that they’re uncertain about what they would do if they came across inappropriate material on their games console. Parents and carers should encourage their children to tell them about anything they have seen or heard that has made them feel uncomfortable or scared.

Parents and carers should report incidents to their internet service provider and in instances of sexual contact to the Child Exploitation and Online Protection Centre (CEOP) using their report abuse button.

CEOP REPORT
ceop.police.uk

Some sites also provide a direct link to CEOP, usually through a red button. If you/your child encounter content online that you think might be illegal, there are two things you can do. Firstly, report it to the Internet Watch Foundation (IWF). Again some sites may provide a direct link to the IWF. Secondly, report the content to your internet service provider.

Further help is available at the following websites

Wii:
http://www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

XBox: http://www.xbox.com/en-GB/support/xbox360/familysettings/consolefamilysettings.htm

Nintendo DS: http://www.nintendo.com/consumer/systems/ds/dsprivacy.jsp

Sony Playstation: http://www.us.playstation.com/support

IWF: http://www.iwf.org.uk/reporting.htm

ThinkuKnow: http://www.thinkuknow.co.uk/parents/faq/gaming.aspx

Chatdanger: http://www.chatdanger.com/

CEOP: http://www.ceop.gov.uk/reportabuse/index.asp

KnowITAll: http://www.childnet-int.org/kia/

Information from:http://consumers.ofcom.org.uk/2009/10/parental-controls-for-games-consoles-and-portable-media-players/