A parents' guide to filtering technologies

GET WITH IT!

understanding the benefits
of filtering to help protect
your child online

Contents Page

1. Introduction:
A guide to filtering technologies

This booklet is about helping you

Children today are growing up with many technologies that weren't around when their parents were young: the mobile phone, the games console, the personal computer, and the internet.

These technologies benefit children's lives in many ways. The internet, in particular, opens up a new world for children: for contact with friends and family, for entertainment, for education and learning.

When children ask a question (like, 'Is the moon made of cheese?'), they can probably find an answer on the internet.

Over the last couple of years, children have begun using the internet at younger and younger ages. This is a good thing. The internet will become more – not less – important in the world as they grow up. Used from an early age, the internet can help children develop some of the skills and knowledge they'll need as adults.

Unfortunately, not everyone who uses the internet has good intentions. The internet carries material that can upset or even harm children.

This poses difficult questions to parents. How do I make sure my children are using the internet safely? How do I know that what they read, see and hear on the internet is suitable? Who are my children communicating with online?

It is natural to be concerned for your children's safety in all areas of life. The internet is no different. Parents face two main challenges online:

1: Protecting children from what is bad on the internet

2: Guiding them to what is good, fun, and educational

These challenges aren't new. For decades, parents have had to make sure their children don't watch late-night television, or watch videos meant for 15 or 18 year-olds. The challenge with the internet is basically the same, stopping children from seeing things they shouldn't.

There was an easy solution with television, change channel or switch it off.

The internet can seem more difficult, especially if you're not sure how to use it yourself. Switching it off can seem the easy option. But it will mean your children lose out on a world of valuable information, learning, and entertainment.

What's more, you don't need to do it. There are a number of easy steps you can take to make your children's internet use safer.

This guide will help you by explaining the following:

1: The parent's role in making children's internet use safer

2: The internet protections that are already on your computer and how to switch them on

3: How 'filtering software' can help protect children online, how it works, and where you can get it

As you read this guide, please remember the following: filtering software offers an added layer of protection when your children are using a computer, **but it is not a substitute for parents' vigilance.**

2. Possible dangers to children on the internet

The possible dangers to children on the internet:

- Inappropriate content: pornography, racist, hate, and violent material, or content that is simply aimed at a grown-up audience (a bit like late-night television)
- Computer viruses: they can destroy information on your computer or stop the computer working properly
- Spam emails. These are like junk mail. You did not ask to receive them and they are not from a person you know. Opening them, especially if they carry attachments, can introduce viruses or inappropriate content to your computer
- Social-networking websites, chat-rooms and instant messaging. These are programs that allow people to send messages to each other, like in a conversation. Sometimes adults use them to try to make contact with children, often by pretending to be children themselves. Such people are known as online predators
- Scams, fraud, phishing. These can be attempts to con people out of money or into giving away their financial information

It is impossible to list every potential danger online. As in any walk of life, a parent's vigilance is crucial to ensure children are safe. If you or your children ever come across content on the internet that you suspect to be illegal, please report it using the confidential www.hotline.ie service

3. About filtering software

What is filtering software?

Filtering software is a program that 'filters' out and blocks inappropriate internet content before children can see it on the computer screen.

To access the internet you need two things. The first is an internet connection. This allows you to go online. The second is a program called a web-browser. This allows you to search for and see websites. Filtering software stands between the two of these. It can block inappropriate content that comes through the connection from showing up on the computer screen.

To connect to the internet you need an ISP. This stands for Internet Service Provider – the company that supplies you with a connection to the internet (e.g. Eircom, Vodafone, UPC, Clearwire, UTV Internet). You can phone or email your ISP to ask about the parental controls on their services.

Often, children who see inappropriate content on the internet do not go looking for it. Children can be misled online. Websites with innocent-sounding names can carry pornography, for example. If a child clicks on such a website, the filtering software can block the content before the child sees it.

Browsing the web is not the only thing you can do on the internet. In addition to your web-browser, other software can allow you to send emails and instant messages, share files through peer-to-peer (P2P) networks, or make voice calls over the internet (VoIP). Filters for the web may not work with these other services.

Filtering software can help you in the following ways:

- Gives you – and not your children – overall control of the computer
- Blocks inappropriate content from appearing on the computer screen
- Records a list of all websites that your child has visited, so you can see if they are suitable or not. This list is called an 'Activity Log'
- Limits the amount of time your child spends on the internet. If you decide you want your children to spend no more than one hour a day online, you can use filtering software to stop them using the internet for longer than this
- Reduces the risk of computer viruses by restricting the websites your children can visit. It also limits the types of programs and attachments they can download onto the computer
- Protects personal information on the computer. It can stop children accidentally sending out financial information stored on the computer
- Blocks applications (programs) that you do not want your children to use, e.g. videogames, instant messaging
- Blocks file sharing. This means taking a piece of content (e.g. a music file) off one computer and transferring it to another
- Allows you to set different 'filter levels' depending on the age of your children (e.g. the 'filter' levels for a 10 year-old can be stricter than those for a teenager)

What is the best filtering software?

The answer is simple. You, the parent, are the best filtering software for your children. No filtering software guarantees to block 100% of inappropriate content. There are ways to get around the 'blocks' put up by filtering software. Many people go to great lengths to disguise inappropriate content as innocent.

Close parental supervision of your children's internet use is the best way to fight this.

# 4. Advice to parents on supervising children's internet use

How can I supervise my children's internet use?

Learn how to use the technology yourself. In this case, knowledge really is power. You'll find it difficult to supervise your children's internet activity if they know more about the technology than you do.

Computers and the internet can look hard to use at first glance. In fact, they are easy to use – after a little time, patience and practice. You can teach yourself many programs if you follow the instructions on-screen. Also, computer courses – from beginners to advanced – are available around the country.

Learning to use the technology will have two benefits. First, you can help make your children's internet experience safer. Second, you can make your own internet experience more enjoyable, especially as you will be able to share online activities with your children.

As your children grow older, they will probably want to surf (search) the internet on their own. You will have to make a decision then. How much privacy do you allow your children while still knowing that their internet use is safe?
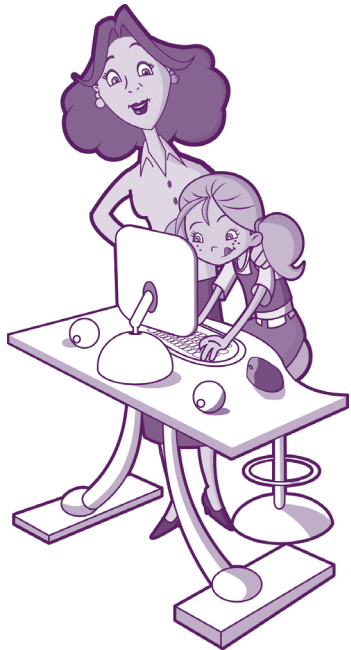
Steps parents can take to make their children's internet use safer:

- Learn how to use the computer and the internet yourself. It'll be difficult to supervise your children's internet use if you cannot use the technology
- Make surfing the internet a family activity, especially with younger children
- Set family rules for using the internet. Explain what your children can look up, when they can use the internet and for how long, and the amount of personal information they can give away online (as little as possible, especially for younger children)
- Keep the rules short and simple for younger children. Otherwise they'll get confused
- Take an interest in what your children do online. Talk to them about the websites they visit, the subjects they look up, and – most importantly – with whom they communicate online
- Keep the computer in a busy room in the house, not hidden away in a bedroom
- Talk to your children if their behaviour changes and you suspect it has something to do with their use of the internet (e.g. online bullying, when someone sends them nasty messages)
- Encourage them to talk to you if they see or read anything on the internet that makes them uncomfortable or upsets them
- Never allow your children to go alone to meet an online friend in real life. If you do allow your children to meet friends they have made online, make sure a responsible adult accompanies them and that the meeting takes place in a busy public area. If the person is different to how they described themselves online (e.g. a grown-up, after claiming online they were a child), leave immediately. Report any alarming incidents to the gardaí

A child's own filtering software is 'common sense'. Teach them the values of good internet use.

Rules for safe internet use by children:

- Children should not give away personal information online, especially on public websites or to people they do not know. Personal information includes their name, address, phone number, email address, photographs of themselves, or any family financial information such as bank account numbers. Check the amount of information your children show to the public if they use social-networking websites (these are websites where teenagers can meet online and chat to each other. Popular websites include Facebook, Bebo or MySpace)
- Children should ask your permission if they want to use chat-rooms or instant messaging. Many chat-rooms are unmonitored – that means, no adult is responsible for making sure the chat is suitable and safe. Sometimes, online predators will try to make contact with children through chat-rooms and instant messaging
- Agree with your children whom they can email (e.g. friends, family). They should talk to you if anyone else tries to contact them online. It is very important that they tell you immediately if a stranger online asks to meet up with them
- Children should not open attachments in an email without asking parents, especially if the email is from someone they do not know. Such attachments can contain viruses or inappropriate content
- Tell children the types of websites (e.g. educational) they can visit
- Tell children the times and for how long they can use the internet

5. Use of filtering technologies:

What protections are on my computer already?

In most cases, your computer will already have 'filters' that you can use for free. All you have to do is switch them on.

- On the computer operating systems

Every computer needs a program called an operating system. This program manages the hardware and the software of the computer. The operating system is at work when you click an icon to run a piece of software or set a disc playing in the CD-ROM drive. The most common operating system on personal computers is Microsoft Windows. The new version of Windows – 7 – comes with Parental Controls just like its predecessor - Vista. The earlier version of Windows XP did not have dedicated parental controls but did provide account and password protections for children's account. On Apple Macintosh computers, the operating system is called either OS X Tiger or OS X Leopard (the name may change as newer versions come out). It, too, has Parental Controls.

How to set the Parental Controls on Windows 7:

- When your computer boots up (switches on), click the 'Windows 7' icon at the bottom left-hand corner of the screen
- A menu of applications and options will rise from the 'Windows 7' icon. Click 'Control Panel'
- Click on 'User Accounts and Family Safety' settings
- You will now have access to the Parental Controls
- Through the Parental Controls you can limit the times and how long your children can use the computer, the types of games they can play, and the number of websites they can visit
- You can also read an activity report, which will outline how your children have been using the computer

*Windows Vista follows the same procedure for setting parental controls.

How to set password controls on Windows XP:

XP is an earlier version of Windows. It doesn't have a dedicated Parental Control option, but it does have account and password protections that can restrict a child's use of the computer.

- Click the 'Start' icon at the bottom left-hand corner of the screen
- Click 'Control Panel'
- Click 'User Accounts'
- You will see options to 'Change an account' or 'Create a new account'
- You should then set yourself up with a password protected 'Administrator' account
- Next set up 'Guest' accounts for your children
- With an 'Administrator' account, you have most control over the computer and can set boundaries to how your children use their 'Guest' accounts

How to set the Parental Controls on OS X:

- When the computer boots up, click 'System Preferences'
- Click 'Accounts'
- Here you can set up accounts for yourself and your children
- Your account should have overall password-protected control of the computer
- Select your children's accounts and click on 'Parental Controls'
- You can then set boundaries to how your children use the computer, e.g. by setting up a safe-list of people they can email, or by restricting the computer programs they can access
- In 'Parental Controls' you can also restrict your children's use of the Macintosh web-browser, Safari

- On web browsers

Web-browsers are computer programs that allow you to explore the Internet. On personal computers, the most popular web-browser is Microsoft's Internet Explorer. Mozilla Firefox and Google Chrome are also popular web-browsers. Safari is the main web-browser on Apple Macintosh computers, but it is available on the personal computer also.

These programs allow you to block certain websites and pop-ups. (Pop-ups are small advertisements that literally 'pop-up' on the screen when you go to some websites. Most are harmless and can be removed by clicking on the X at the top right-hand corner of the pop-up. Some, though, can lead to inappropriate content.)

How to set the filters on Internet Explorer:

- Go to the menu at the top of the screen. Click 'Tools'
- A smaller menu will drop down. Click 'Internet Options'
- Click 'Content'
- Click 'Content Advisor'
- In the 'Content Advisor' menu, you have options to block particular websites, block websites that contain unsuitable words, or set password controls

How to set the filters on Mozilla Firefox:

- Go to the menu at the top of the screen. Click 'Tools'
- A smaller menu will drop down. Click 'Options'
- Click 'Web-features'
- In 'Web-features' you can block pop-ups
- Another option is to click 'Privacy'. Here you can set the history (a record of which websites have been visited) and add passwords

How to set the Parental Controls on Safari:

- Log onto the computer with your 'Administrator' account – an account that gives you overall password control of the computer
- Open the Safari web-browser
- Click 'Preferences'
- Click 'Security'
- Here you will have an option to 'Enable Parental Controls'
- You can list the websites that your children can access in the 'Bookmarks bar'
- When your children log on, they will be blocked from visiting any other websites unless you authorise them on your 'Administrator' account

*Google Chrome: Users of Google Chrome should note that this web browser doesn't have Parental Controls and that a third party web filter should be used in this case. Please see page 22 of this booklet.

The examples above are simple to use and free. But remember two things. First, they do not guarantee to block all inappropriate content. Second, the filters and controls can be switched off as easily as they were switched on, especially if your children gain access to your account password. Check the settings regularly if you suspect that your children know how to switch them off.
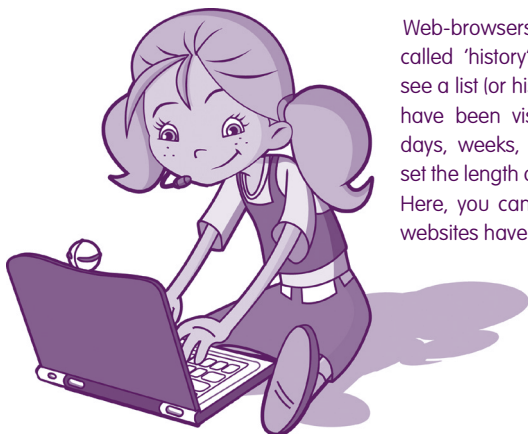
Web-browsers have a useful feature called 'history'. This allows you to see a list (or history) of websites that have been visited in the last few days, weeks, or months. (You can set the length of the history yourself.) Here, you can see if inappropriate websites have been visited.

- On search-engines

The internet contains millions of pages of information on all kinds of subjects. The easiest way to find what you're looking for is through a search-engine.

A search-engine is an online service that allows you to type in words on a subject of interest (e.g. volcanoes and eruptions). It will then search the internet for websites that contain those words. You click on the link to whichever website interests you.

The most popular search-engines are Google (www.google.ie), Yahoo (www.yahoo.com), and Microsoft's Bing (www.bing.com).

Search-engines are useful ways to find information. They are also one of the easiest ways to find inappropriate content. For example, a search for the word 'porn' through Google will return over 91 million results.

If you allow your children to use search-engines, you can switch on the 'safe-search' option. This is a filter to block inappropriate content from showing up in search results. (However, no search-engine guarantees to block all inappropriate content from children.)

How to set the filters on Google:

- Open your web-browser. Type www.google.ie into the navigation tool-bar at the top of the screen
- Click the link for 'Search Settings', which is at the top right of google.ie webpage.
- Near the bottom of the page, you will see three options for 'safe-search filtering'
- Click the option to 'Use strict filtering'. This will block websites with inappropriate text or images from showing up in search results
- Click the option to 'Save preferences'. This means the search-engine will remember to use strict filtering the next time someone tries a word search

How to set the filters on Yahoo:

- Open your web-browser. Type www.yahoo.ie into the navigation tool-bar at the top of the screen
- Click 'Web search'
- Click on the word 'More'
- Click 'Preferences'
- Click the option to 'Edit' the level of safe-search
- Here you can tell the search-engine to block inappropriate content
- Click 'Save', so the search-engine will remember to use strict filtering the next time somebody uses a word search

How to set the filters on Bing:

- Open your web-browser. Type www.bing.ie into the navigation tool-bar at the top of the screen
- Click the link for 'Preferences', which is at the top right of webpage.
- At the top of the page, you will see three options for 'safe-search filtering'
- Click the option 'Strict'. This will block websites with inappropriate text or images from showing up in search results
- Click the option to 'Save settings'. This means the search-engine will remember to use strict filtering the next time someone tries a word search

- On games consoles

Video games consoles have come along way since the mid seventies when Atari launched the hugely popular Pong console. Now not only can you play games but you can watch DVDs/Blu Ray, listen to CDs/ MP3s and you can access the internet to play different people from around the world or just simply browse the web. The following are guides to help you set up Parental Controls on the Sony Playstation 3 (PS3) and the Nintendo Wii. Microsoft's Xbox 360 doesn't have web browsing capabilities.

Playstation 3: The PS3 includes parental control settings that restrict playing content that would have a mature theme, whether it's a game, a video or using the internet. All parental controls are restricted by one password.

How to set a password on a Playstation 3:

- Start your PS3 and enter the main menu.
- Scroll left and select 'Settings'.
- Scroll down and select 'Security Settings'.
- Select 'Change Password'.
- Follow the on-screen instructions to set the password

* The password is set to 0000 by default at the time of purchase.

How to restrict web browsing on a Playstation 3:

- Start your PS3 and enter the main menu.
- Scroll left and select 'Settings'.
- Scroll down and select 'Security Settings'.
- Select 'Internet Browser Start Control'.
- Select 'Off', which will disable the use the browser or
- Select 'On', which will enable access to the browser but the password is required.

You can use web filtering software on a PS3, which will automatically block inappropriate website. We discuss the different software on page 22.

For instructions on other parental controls, such as restricting Games, DVDs and Blu Ray. Please see the following link:
http://manuals.playstation.net/document/en/ps3/current/basicoperations/parentallock.html

Nintendo Wii: Unlike the PS3, the Nintendo Wii isn't ready for web browsing straight out of the box. In order to use its web browsing feature you need to download the Internet Channel from Nintendo's Wii Shop.

How to restrict web browsing on a Nintendo Wii

- Start your Wii and enter the main menu
- Access the Wii System Settings
- Click on the blue arrow once to reach the Wii System Settings 2 menu options
- Select the right arrow twice to reach the third page, then select 'Parental Controls.'
- Select 'Restrict the use of Internet Channel'
- Select 'Yes'
- When you are finished, select 'OK' to save your settings and return to the Start Page

---

For instructions on other parental controls, such as restricting Games. Please see the following link: http://www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

- On Handheld devices

This section will look at the different handheld devices such as Sony's PSP, Nintendo's DSi and the Apple iPhone.

<u>Sony PSP:</u> To the set the Internet controls on the PSP is similar to the PS3 but you cannot use web filtering software it like you can on the PS3.

How to restrict web browsing on a PSP:

- Start your PSP and enter the main menu.
- Scroll left and select 'Settings'.
- Scroll down and select 'Security Settings'.
- Select 'Change Password' and insert the default password - 0000.
- Input your new password and press X to save
- After you have sent your new password select 'Internet Browser Start Control'.
- Select 'Off', which will disable the use the browser or
- Select 'On', which will enable access to the browser but the password is required.

For instructions on other parental controls, please see the following link:
http://manuals.playstation.net/document/en/psp/current/settings/parental.html

<u>Nintendo DSi:</u> Most DSi's come with a browser preinstalled but if it isn't, it can be downloaded from the Nintendo DSi Shop. To disable the use of the internet on the DSi, you'll need to first set a pin number:

Setting a pin number on a DSi:

- On the Nintendo DSi Menu, use the stylus to select the Settings icon.
- Select the right arrow twice to reach the third page, then select 'Prental Controls.'
- Select 'Yes,' 'Next,' then 'OK' to reach the PIN screen.
- Select 'Next,' enter a four-digit PIN, then tap 'OK.' Enter the PIN again to confirm it, then tap 'OK' again.
- Tap the up/down arrows to scroll through the secret questions. When the desired question is displayed, select 'OK' to continue.
- Select 'OK' again, use the on-screen keyboard to enter an answer to the secret question, then select 'OK.' The answer must be six or more characters long.

On the Nintendo DSi you can either completely block access to browsing the internet or you can restrict access to inappropriate content. The following guides can help you to do both:

How to block access to browsing the internet:

- On the Nintendo DSi Menu, use the stylus to select the 'Settings' icon.
- Select the right arrow twice to reach the third page, then select 'Parental Controls.'
- Select 'Restrict the use of Nintendo DSi Browser'
- Select 'Yes'
- You will be then asked to provide the pin which you should have already set up.
- When you are finished, select 'OK' to save your settings and return to the Start Page

The web content filtering software that Nintendo exclusively uses was designed by a company called Astaro and it is free-of-charge. This service, when enabled, is capable of blocking over 60 million

websites that contain inappropriate or undesirable content such as pornography, illegal drugs, weapons, and violence.

For a complete list of all blocked categories, please visit http://www.astaro.com/ds-content-filter.

Blocked categories may change periodically. Parents please note that use of the Astaro filtering may not block all websites you consider unsuitable for your child so it is important for you to participate in and monitor your child's use of the Nintendo DSi Browser.

How to set up the Astaro content filtering software on a DSi:

- On the main menu of the Nintendo DSi, tap the 'Web' icon to launch the Nintendo DSi Browser.
- On the the start page, tap 'Settings.'
- Scroll down through the settings until you reach a button labeled 'Proxy,' and click on it to reach the 'Proxy settings' menu.
- Select 'Use proxy' to highlight the proxy fields.
- Enter in the following proxy information (if it isn't already there):
- In the 'Server' field, enter: ds-content-filter.astaro.com
- In the 'Port' field, enter: 8080
- If you want to use the proxy to access HTTPS (secure web sites), select 'Use for HTTPS.' (This is optional.)
- Setting a username and password will require them to be entered to unlock the proxy settings in the future. To set this, select 'Use proxy authentication.' Then, enter a username and password into the appropriate boxes. (This is optional.)
- When you are finished, select 'OK' to save your settings and return to the Start Page

---

For more information on other parental controls please visit the the following link: http://www.nintendo.com/consumer/systems/dsi/en_na/settingsParentalControls.jsp#Topic02

Apple iPhone: The iPhone is equipped with parental controls to enable parents to deactivate different features on the device

including access to the internet. Through the settings feature on the iPhone parents can set up a special pin code and then disable internet access. When this is done users cannot browse the internet or access web clips. Other applications on the iPhone can also be deactivated in the same way including Youtube and the itunes wifi music store.

Further information about the restrictions can be accessed at: http://manuals.info.apple.com/en_US/iPhone_User_Guide.pdf

To set up parental controls on different makes or models of mobile phones please enquire at the point of purchase or consult the manufacturers website for more information.

6. Buying or downloading filtering software

What are the types of filtering software I can buy or download?

Parental supervision is the most important filtering software. The next most important is your children's common sense – through teaching them the rules and values of safe internet use. You can also set up basic filters on your web-browser, search-engines and newer operating systems.

But if you want extra security for your children online, you could consider buying or downloading filtering software.

You can buy filtering software in computer shops and in some supermarkets. Ask the retailer for advice on the best products.

You can also download filtering software from the internet. Some of it is free; some of it you'll have to buy.

Many of the companies that charge a fee also offer 'free trials', e.g. a 14-day free trial. You can use the free trial to test the filtering software. If it does the job you want, you can then buy a version that will stay on your computer permanently.

You do not need technical experience to put filtering software on your computer. When you download filtering software from the internet, or buy it on a CD-ROM in a shop, you will be given some simple on-screen instructions. Most of the time, you have only to click 'Ok' to install the software. Then click 'I agree' to the terms and conditions of the software. The computer will do most of the rest by itself.

Don't be put off by the terms and conditions. When you buy a film on DVD, you automatically agree to some terms and conditions, e.g. that you will not copy the film. This is just the computer version of that.

Filtering software packages:

Below are some filtering software packages that you can find either in computer shops or on the internet. If you buy software in a shop, ask the retailer for advice on the best package for your needs. If you buy online, you can often get a 'free trial' to try before you buy.

- Reassure Me: www.reassureme.com

- CyberPatrol: www.cyberpatrol.com

- NetNanny: www.netnanny.com

- CensorNet: www.censornet.com

- SafeEyes: www.safeeyes.com

Remember, computers are commonplace. Your children won't always be using the computer at home. Computers at school or at their friend's house might not have filtering software. If their friends have laptops, they may gain access to wireless internet at certain public places where no one is monitoring the websites they visit. Therefore, it is important your children know the rules for safe internet use no matter where they are online.

This is particularly important if your children use internet cafés. Adults routinely use internet cafés, so the computers there may not be set to filter out content that would be inappropriate for children. Also, some internet cafés offer networked games – games where people sitting at different computers play against each other. Some of these games are violent and inappropriate for children. You should check with an assistant at the internet café to find out if there are rules for computer use by children.

The EU's Safer Internet Programme Parental Controls Benchmarking Study

The safer internet programme conducts an expert, vendor/supplier-independent, objective assessment of the filtering software and services currently available. The study was carried out through an annual benchmarking exercise of approximately 30 parental control products or services repeated over 3 years.

You can view the results from these studies from the following link

http://www.sipbench.eu/index.cfm

The weaknesses of filtering software

Filtering software can help to make internet use safer for your children. But it is not perfect. No filtering software guarantees to block all inappropriate content, though some programs are better than others. In the shops, ask for advice. On the internet, use the free trials to test the software.

Some filtering software programs can be too strict. They can block innocent content, mistaking it as inappropriate. For example, they can block children from researching a history essay on the Second World War because the search leads to websites that describe violence.

Filtering software can act as a censor when adults use the computer.

Some programs are good at recognising and blocking inappropriate content on English language websites, but weak at doing so on websites in other languages.

In some cases, the program may not block a website where the nature of the content has changed over time.

Filters that can be switched on can be switched off too. As children grow older, they become more sophisticated in their computer use. In a small number of cases, they will be able to switch off the filtering software and cover their tracks. You will know this is happening only if you learn how to use the computer and the software yourself.
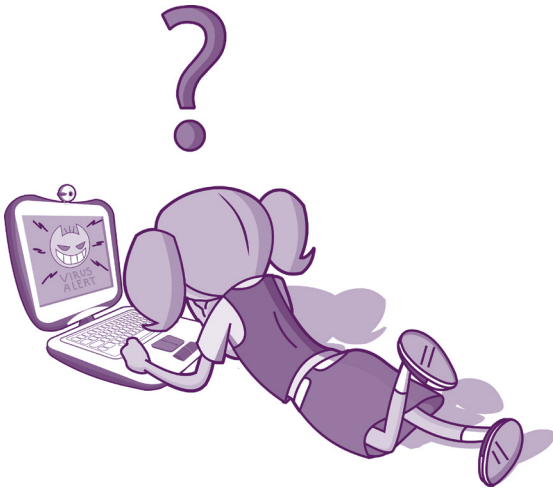
Anti-virus and anti-spyware software

Another problem you may come across is computer viruses. A virus is a malicious piece of software that can do great damage to a personal computer. The more serious viruses will stop your computer working properly or may delete information off it. Many computers are infected with viruses from other people's disks or memory sticks, or when users open the attachments of spam emails. Viruses can also be downloaded onto computers when users visit certain websites, e.g. pornography websites. As well as using filtering software, you should protect your family computer with anti-virus software and make sure that your subscription to it is kept up to date. You can buy anti-virus software in most computer shops. Some examples of anti-virus software are as follows:

Anti-virus software:

- **Norton Antivirus**
- **McAfee**
- **BitDefender**

Computers can also be infected with spyware, which will try to collect personal information from your computer without your permission. Some spyware (or adware, in this case) can use the personal information to target advertisements at your computer. This can be annoying and disrupt the normal working of your computer. More serious forms of spyware can try to collect financial information from your computer and send it to someone else's machine.

Spyware often presents itself as a useful piece of software – e.g. a program to make web-browsing faster – to trick people into downloading it. As a general rule for internet use, you should never download any program or content unless you are sure it comes from a reliable source.

Some anti-spyware programs are available for free on the internet and they work well. But be careful when downloading any such programs. Some of them are fake: instead of protecting your computer they will actually infect it with spyware. Your first step should be to check if your anti-virus software also has features to protect against spyware.

7. Useful web sites

Please note that these links are intended as assistance and the Office for Internet Safety does not accept responsibility or endorse any of the websites listed nor the information that is contained within them.

You can get further information on safe internet use from the following websites:

Irish websites:

Office for Internet Safety:
www.internetsafety.ie

Tips on internet safety:
www.webwise.ie

The Professional Development Service for Teachers Technology in Education: www.pdsttechnologyineducation.ie

A website devoted to providing a portal for young people to show their support for victims of cyber bullying:
www.watchyourspace.ie

To report content you suspect to be illegal, particularly instances of child pornography:
www.hotline.ie

Child safety issues:
www.childline.ie

Child support charity:
www.barnardos.ie

A national awareness campaign to raise digital safety:
www.makeitsecure.org

Advice for parents:
www.rollercoaster.ie

International websites:

European network for internet safety: www.saferinternet.org

The Child Exploitation and Online Protection Centre (based in the United Kingdom):
www.thinkuknow.co.uk

ChildNet, a not-for-profit organisation to promote internet safety:
www.childnet-int.org

A website, from ChildNet, that discusses the potential dangers of online chat-rooms: www.chatdanger.com

The American 'National Academies' online resource for parents: www.nap.edu/netsafekids

A European project to promote research into children's use of the internet: www.eukidsonline.net

A family guide to online safety: www.safekids.com

A not-for-profit information resource for child safety online: www.netfamilynews.org

For children:

Ask About Ireland is your place to find answers about Ireland. Our countryside, our heritage, the way we work and play. Here you'll have unique access to new information, rare images and documents from Irish public libraries, museums and archives: http://www.askaboutireland.ie
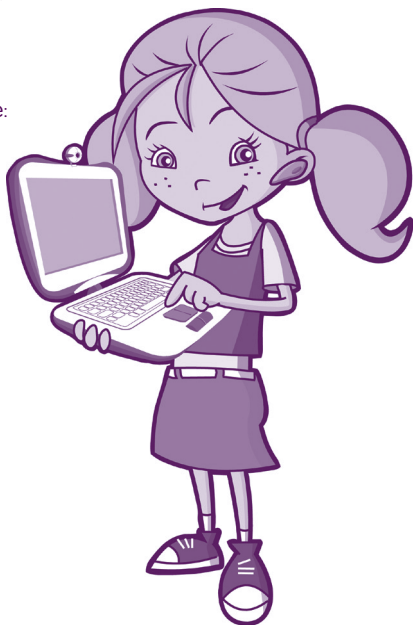
'Get With IT!' Series

The 'Get With IT!' series of booklets is available on the publications section of the Office for Internet Safety website www.internetsafety.ie .

There are four booklets in the series:

A parents' guide to new media technologies,
A parents' guide to filtering technologies,
A parents' guide to social-networking websites, and
A guide to cyberbullying

Hard copies of the booklets are available on request from the Office for Internet Safety at:

Freefone: 1800 24 25 95
Email: getwithit@justice.ie

GET WITH IT!

This booklet is about helping you

The world of new media technologies, particularly the internet, is generally one of fun, learning and creativity. However, parents sometimes worry about the dangers that these technologies hold for their children, from inappropriate content to the risks posed by predatory adults online.

This booklet is intended to advise parents on the benefits (and the shortcomings) of filtering technologies. It outlines how they work and encourages parents to use them as part of a package of measures to block inappropriate content from their children.

The message is simple, FILTER IT, it all helps to keep children safer.