Internet Safety

Considerations for keeping your children safe when using the internet

Hand-out for Parents

Version: Rev 07 - 2015

Presenter: schoolswebsites.ie

The following topics are covered in this handout:

- Cyber Bullying
- Sexual Predators
- Inappropriate content
- Damaged Reputation
- Theft
- Making your mobile device safe
- Putting Restrictions on Apple Devices
- Putting Restrictions on Android Devices
- Browser History
- Blocking Advertisements on Browsers
- Gmail
- Facebook privacy
- Email Scams
- YouTube Safe Searching
- Content Filtering on your Router
- Hotline.ie
- Current legislation
- Important resources

Cyber Bullying:

Tips:

1. Kids should NEVER share passwords with ANYONE – as a parent, you should know your child's passwords
2. Teach them how to use the "block", "ban" and "report" features of the system.
3. If bullying continues – delete the account and start afresh – never giving out details to anyone other than family and real friends.
4. Never respond to rude, harassing, hurtful messages.
5. Report it to www.hotline.ie
6. NEVER OVER REACT when your child talks to you about this.
7. Always maintain channels of communication with your kids

Sexual Predators:

Tips:

1. Periodically check you child's social media presence. If allowed do it with your child. If not, use duckduckgo.com to search for your child's name.
2. Your child should NEVER post ANY information that could give a hint about geographical location: address; phone numbers etc.
3. You as a parent need to learn about privacy settings on the social media systems your child is using.
4. You need to learn the 'text-speak' that your children are using. For example "POS" = "Parent over Shoulder" and "LMIRL" means "Let's meet in real life".
   http://www.webopedia.com/quick_ref/textmessageabbreviations.asp
5. There is no substitute for Parental Supervision. NEVER allow private internet access.
6. You child should NEVER 'friend' someone WHO THEY DON'T KNOW IN REAL LIFE. If you child has more than a couple of dozen friends then you need to talk to them.
7. Kids should report anything they think is inappropriate: www.hotline.ie

Inappropriate Content:

Tips:

1. Never allow private internet access
2. Check browser history
3. Talk to your children
4. Make sure youtube settings are set for age appropriate content: protected vs unprotected
5. Use your wireless router to filter out dodgy sites: remember to put in foreign language equivalents. More on this later
6. Install filtering software on your devices:
   a. Windows Family Safety: familysafety.microsoft.com
   b. AVG Family Safety: http://www.avg.com/us-en/avg-family-safety (see 'Making your mobile device safe for more details)

Damaged Reputation:

Tips:

1. Get your kids to understand that even if they delete something from their online profiles – others WILL have already copied it.
2. Your child needs to tell their own friends NEVER to take images that might cause embarrassment in the future.
3. Talk to your kids about the future possible consequences of stupid posts they make now.

Theft:

Tips:

1. Always intelligently look at EVERY link you are about to click on BEFORE you click on it.
2. Never install apps or software that you haven't checked the reviews of. Never install anything that doesn't have hundreds of good reviews.
3. Dis-associate your credit cards from you Play Store / iTunes account

Making your mobile device safe

AVG Family Safety
AVG Family Safety is a free app for iPod touch, iPad and iPhone. It will automatically block websites categorized as pornography or malware. But you can also add websites to a block list. So if you want to block YouTube, just add it to the block list. Be sure to add both the full YouTube web address and the mobile version (m.youtube.com). There is also a tie-in with their AVG Family Safety service for your family computer. If you already use that service, then the app can connect and you'll get more advanced filtering features.

Pros: No registration needed, easy to use, can choose the default search engine
Cons: a few bugs, and need to specifically add most sites to block especially for younger kids

http://itunes.apple.com/us/app/avg-family-safety/id423567709?mt=8

K9 Web Protection browser
K9 Web Web Protection is a free app for iPod touch, iPad and iPhone. It is also available for Android devices. It will block adult and potentially offensive or malicious sites. You can view the browsing history to see which sites were blocked (but note that your child could also view and then clear this history). The browser uses its own Safe Search capabilities. If you want to quickly block YouTube, this will do the trick.

Pros: Easiest to use with no registration or passwords needed
Cons: No customization available.

iTunes: http://itunes.apple.com/app/k9-web-protection-browser/id407657840
Android: https://play.google.com/store/apps/details?id=com.bluecoat.k9.android&hl=en

McGruff Safe Guard Mobile Browser
McGruff Safe Guard is a free app for iPod touch, iPad and iPhone. It restricts websites by age range – either Child (1-12) or Teen (13-17). With a $1 upgrade you'll get more features such as the ability to pick categories and sites to allow or

deny. If your main goal is to block YouTube, you don't need the upgrade as it is blocked for both the child and teen age ranges. I did find though that my child's school website was blocked in the 1-12 range which was surprising. If I were to set this up on her device I'd definitely splurge and pay $1 for the full version.

Pros: Easy to set up; daily e-mail report (can unsubscribe if desired), parent can lock safe search
Cons: Would be useful if the parent e-mail contained the URL of the sites that were blocked (need the full version for that).

http://itunes.apple.com/us/app/mcgruff-safeguard-browser/id493861295?mt=8

MobSafety Ranger Browser
Ranger Browser is a free app for iPod touch, iPad and iPhone. It is also available for Android devices. This app is a bit different from the others. You register on their website and set up an account with your child's name. Then choose the level of content filtering per child – high, medium or low. You can, in theory, choose to block everything, and then just allow certain websites if you want to really limit things. However when I tried this, it did not work. If they could fix a few issues this app could be a good choice, but as-is I was able to view sites from search that should have been blocked.

Pros: Time limit settings; ability to customize and add websites to always block or allow; web page for parents to view history.
Cons: Could not find documentation in the app or their website; some of the settings did not seem to work – I blocked all sites except allowed one on the "whitelist" and I could still get to other sites using Search.

iTunes: http://itunes.apple.com/us/app/ranger-browser-safe-internet/id406480823?mt=8
Android: https://play.google.com/store/apps/details?id=com.gpit.android.safe.Ranger&hl=en

Putting Restrictions on Apple Devices

Here are instructions for setting parental control restrictions on an iPod touch or iPad. This will also work on an iPhone. If you are "locking down" your child's device and installing a kid-safe browser (see page 1 above), then install the kid-safe browser first. Then follow these steps.

1. From the child's iPod or iPad, go to **Settings > General > Restrictions.**

(these two screenshots are from an iPhone; but should look about the same on your child's device)

2. If you have already set up restrictions, you'll be prompted for the passcode. If not, choose **Enable Restrictions** and enter a passcode. Be sure to use a 4-digit passcode that you will remember and your kids will not guess.

3. Turn YouTube and Safari to the OFF position. In addition, set Installing Apps and Deleting Apps into the OFF position as well (this will prevent your child from adding these Apps back to the device. If you install a kid safe browser, the restriction for Deleting apps will prevent them from deleting the app you install). Once done the screen should look like this:

4. That's it! Just be sure to remember that 4-digit restriction passcode. You will need it to go back and make adjustments such as removing apps or adding new ones. I really recommend this for younger children so you can have a better idea of what they're doing when they are seemingly tethered to their device! And as always, talk with your kids about what they're doing online – parental controls and restrictions are only one side of the equation.

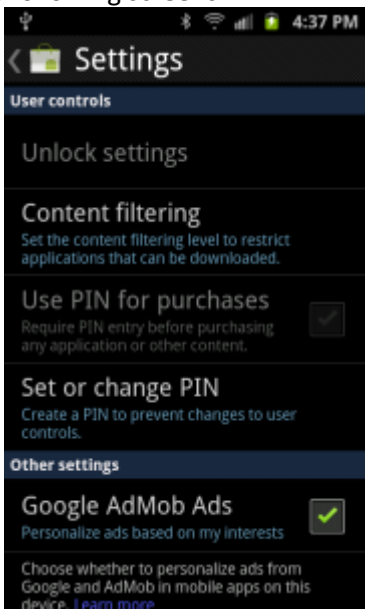
Putting Restrictions on Android Devices

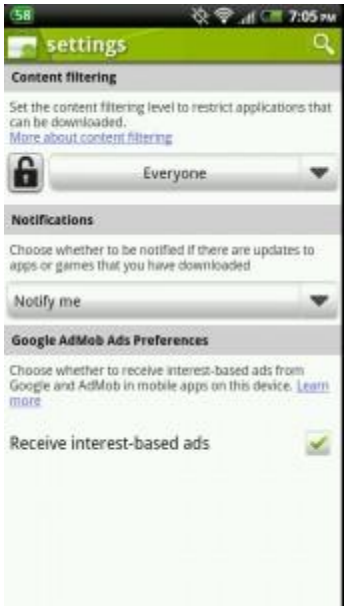
Google Play

Below are the maturity levels that all apps on the Android Market are classified under:

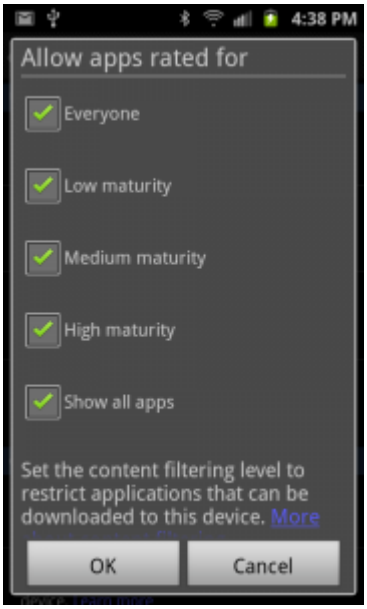
- Everyone
- Low maturity
- Medium maturity
- High maturity

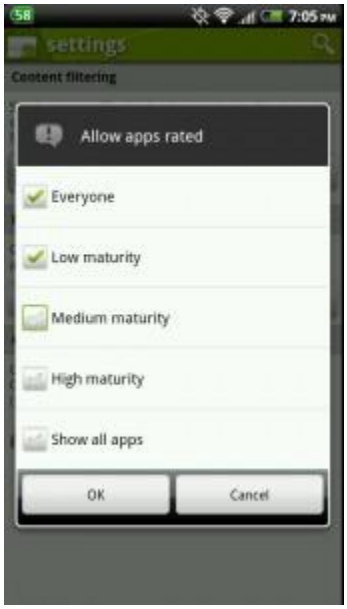
Simply go to your Google Play app and then click the MENU button on your Droid. Then click on the SETTINGS button. You'll then see one of the following screens:





Click on the PULL DOWN menu under Content Filtering and select the maturity level that you (or your child) will be allowed to download. After that, you'll want to click on the LOCK pad icon or the "Set or change PIN" option to setup a PIN password to lockdown the settings you just configured.





That's it! Now the Google Play will only allow you to install the apps that have been deemed appropriate for the maturity level that you have set.

Restricted Profiles

Please refer to this site: http://www.pcadvisor.co.uk/how-to/google-android/3461359/parental-control-on-android/

Browser History

Safari

1. First, open your Safari browser.
2. Click on History in your Safari menu, located at the top of your screen. When the drop-down menu appears your most recent history (the last 10 web pages that you have visited) will appear. In the screenshot below, this section is circled. Clicking on any of these items will take you directly to the respective page.
3. Directly below it you will find the rest of your recorded browsing history, grouped by day into sub-menus. If you have visited more than 10 web pages on the current day, there will also be a sub-menu present labelled "Earlier Today" containing the rest of today's history.

Google Chrome

1. Click the Chrome menu  on the browser toolbar.
2. Select History

Internet Explorer

1. Press the "ctrl" button and then tap the "H" button at the same time. Your history will appear.

Firefox

1. Press the "alt" key. This will display the menus at the top.
2. Click on History

Blocking Advertisements on Browsers

See http://dottech.org/17516/block-ads-in-firefox-internet-explorer-chrome-and-opera-how-to/

Gmail

Android: https://play.google.com/store/apps/details?id=com.google.android.gm&hl=en
iTunes: https://itunes.apple.com/app/gmail/id422689480

How to setup email accounts on your Apple device: http://www.gilsmethod.com/how-to-setup-email-accounts-on-the-ipad

How to setup email accounts on your android device:
As you would expect, Google have made it very easy to set up Gmail through an Android phone or tablet. To setup your Gmail on an Android phone, follow these steps.

1. Open the Settings menu and go to Accounts & sync settings on your device.
2. The Accounts & sync settings screen displays your current sync settings and a list of your current accounts.
3. Touch Add account.
4. Touch Google to add your Google Apps account.
5. Touch Sign in when prompted for your Google Account.
6. Enter your full Google Apps email address as your username, and then enter your password.
7. Select which services you'd like to sync.

Facebook privacy

All things to do with privacy can be found here: https://www.facebook.com/help/445588775451827

Email Scams

How to spot a scam: http://www.wikihow.com/Spot-an-Email-Hoax-or-Phishing-Scam

YouTube Safe Searching

How to Activate Parental Controls for YouTube Safe Search

- To implement the Parental Controls for YouTube, go to YouTube.com and scroll down to the bottom of the page….
- You will see a reference to Safety Mode and it will say OFF...
- Click the Off button to access Parental Control to turn on YouTube Safe Search.
- (Likewise, if you want to turn YouTube Safe Search Off, click the bottom what will now say “On”…)

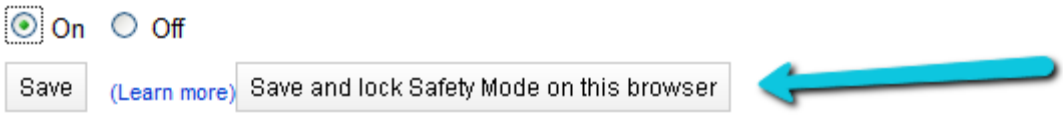
Locking YouTube Safe Search

As you will see, it’s very easy to turn safe search on and off. Therefore, you may want to lock it in order to ensure it is always activated for all family members.

To Lock the Parental Control for YouTube, you will need a Google account. To open a free Google account, go to google.com and click “Sign In” in the top right hand corner of their main website. You will then see the option to create a new account.

Now return to YouTube and scroll down to the bottom of the page to the safety mode link as shown above.

After selecting the “On” button, you will see an option to Lock Safe Search…



Select “Save and lock Safety Mode on this browser”. You will then be required to sign in to your Google account if you have not already done so.

Once Safe Search for YouTube video search is Locked, you can now log out of your account. Unlocking safety mode on YouTube will require you to log into your account. This guarantees that no one else can deactivate the safety setting.

Important: If you have more than one browser on your computer, you will need to follow these steps for each browser. Below is a video that walks you through the process of implementing YouTube Parental Controls that were just explained.
http://www.youtube.com/watch?feature=player_embedded&v=gkI3e0P3S5E

Content Filtering on your Router

If you don’t already have one, it is best to get a router that allows content filtering.
A Content Filtering router will allow you to set a number of different restrictions on the broadband as it enters your home and prior to its distribution to the various devices connected to it throughout the house, (eg tablet, laptop, smartphone, etc).
Log in to your router by following the manufacturer’s instructions or generally, for NETGEAR routers use “routerlogin.net” and for LINKSYS routers use “192.168.1.1”
Once you are logged in you will have the ability to:

1. Set a new router login password
2. Schedule a time for the broadband to be disabled to all devices or some devices, eg night time
3. Schedule a time for the broadband to be enabled to all devices or some devices, eg morning time
4. Block access to any number of selected websites
5. Block access to the internet using certain keywords – the more keywords that are identified the greater the restriction

Hotline.ie

An Garda Síochána do not have a specific police hotline for reporting illegal content on the Internet, thus the Gardaí support that members of the public should report suspected online content to is **Hotline.ie**
In 2014 Hotline.ie processed 4,863 reports and this was 97% above the average of the previous seven years
Hotline.ie is part of a network of 51 Internet Hotlines in 45 countries worldwide.
66% of all reports received in 2014 alleged Child Sexual Abuse Material of which only 10.5% were actually assessed as such. Even so this represents an increase of 148% on 2013
358 reports were determined by Hotline Analysts as illegal under Irish Law, representing 7.4% of all reports processed and assessed by Hotline.ie in 2014
According to Hotline.ie, in 2014, 65% of the victims were children, 33% were in their teens and 2% were infants

Assessment Criteria:

- Trained and internationally certified Hotline Analysts assess reported content, using the best practice and guidelines established in conjunction with the Department of Justice and Equality, the Industry, Law Enforcement and INHOPE
- When assessing whether or not content reported to Hotline.ie (within its remit) is likely illegal under Irish Legislation, the Analysts rely on the Child Trafficking and Pornography Act, 1998 and Prohibition of Incitement to Hatred Act, 1989.
- When Hotline.ie assesses content to be probably illegal, it is simultaneously notified to An Garda Síochána, who may then choose to initiate a criminal investigation and to the appropriate ISPAI Member for removal from public access.
- Only a Court of Law can make a judgement as to whether something is definitively illegal under the law.
- Under the transposition of the EU Directive on Electronic Commerce, ISPs must take action within a reasonable time where identified illegal content is brought to their attention.
- If the content “in itself” is not contrary to law, it is assessed as not illegal and Hotline.ie will not take any further action

If the suspected illegal content is traced to a server located In Ireland:

• The appropriate Irish ISP is identified.

• Hotline.ie issues a notification to An Garda Siochana as the decision to initiate a criminal investigation is a matter for Law Enforcement alone.

• A takedown notice is issued to the appropriate ISP. The ISP is then responsible for the removal of the specified content from their systems while preserving the forensic evidence for the police investigation

If the suspected illegal content is traced to a server outside Irish jurisdiction:

• If an INHOPE Hotline exists in the country of origin, then all technical details, including the determination of Hotline.ie, are forwarded to the appropriate Hotline for processing.

• If the content is located in a country not having an INHOPE presence, Hotline.ie will send the content description and tracing details to the source country through international Law Enforcement channels.

Current legislation

- **The current legislation which governs bullying is as follows:**
    - *Section 2 of the Non Fatal Offences Against the Person Act 1997 sets out the offence of assault as follows:*
        - A person shall be guilty of the offence of assault who, without lawful excuse, intentionally or recklessly causes another to believe on reasonable grounds that he or she is likely immediately to be subjected to any such force or impact, without the consent of the other.

    - *Section 5 of the Non Fatal Offences Against the Person Act 1997 sets out the offence of assault as follows:*
        - A person who, without lawful excuse, makes to another a threat, by any means intending the other to believe it will be carried out, to kill or cause serious harm to that other or a third person shall be guilty of an offence.

    - *Section 10 of the Non Fatal Offences Against the Person Act 1997 sets out the offence of harassment as follows:*
        - Without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence."

If a student is physically beaten or has been put in a reasonable belief of immediate force, the perpetrator will be guilty of assault under section 2 of the 1997 Act.

When a student has threatened to kill or cause serious harm to another and expects that student to believe the threat, this may constitute an offence under section 5 of the 1997 Act.

If a student is harassed by another student it may constitute an offence under section 10 of the 1997 Act.

The **Education Act 1998** states that the responsibility that children's needs are met rests with the schools board of management. Schools in Ireland do not have a set of laws to follow in cases of bullying. Since the Education (Welfare) Act 2000 all schools in Ireland are under a legal duty to have a written code of behaviour. The code of behaviour states, "the standards of behaviour that shall be observed by each student attending the school; the measures that may be taken when a student fails or refuses to observe those standards; procedures and the grounds for removing a suspension imposed in relation to a student". The 2000 Act does not make any reference to the term 'Bullying'.

- The main Irish law dealing with **Data Protection** is the Data Protection (Amendment) Act 2003 and covers all matters of data protection on all types of platforms, whether they are telephone, computer, email, etc. The Acts allow for remedies where a breach or release of information has occurred.
- Another legal remedy available to deal with cyberbullying is the implementation of **Usage Policy**. This would involve contacting the relevant medium or platform on which the cyberbullying is taking place and requesting that all information be removed and that the usage policy is enforced against the perpetrator.
- **Defamation**: A "defamatory statement" means a statement that tends to injure a person's reputation in the eyes of reasonable members of society, Statements made online, whether they appear in social media sites, twitter, e mail etc, are not immune to the laws on defamation. If a defamatory statement is made then civil redress can be claimed through the courts.

- **Injunction**: This is a court order that can either prohibit the publication of certain information or force its removal.

- Ireland has ratified agreements for the promotion and protection of Children's rights. The United Nations Convention on the Rights of the Child 1989 (CRC) is the most significant. The main Article which gives children the right to be educated without violence is Article 19 which states, "parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child"

- Culpability:
  - In civil cases, parents may be held liable or accountable for the actions and conduct of their children in certain circumstances. These circumstances would depend on the facts of each individual case.
  - Schools and similar institutions have an operating duty of care to those in their care. Culpability for cyberbullying can attach to the school or institution in certain limited circumstances. Liability can arise due to the non-implementation of school policies which would allow unmonitored access to the internet through computers or smartphones (and soon smartwatches).

2 bills currently passing through the Seanad are as follows:

- **HARMFUL AND MALICIOUS ELECTRONIC COMMUNICATIONS ACT 2015** (introduced by Senator Lorraine Higgins - recently passed the Second Stage in the Seanad)
  - Summary: An Act to protect against and mitigate harm caused to individuals by all or any digital communications and to provide such individuals with a means of redress for any such offending behaviours directed at them.
  - A person guilty of an offence under this section shall be liable on summary conviction to a fine not exceeding €5,000 or imprisonment for a term not exceeding 12 months or to both
  - The court can order that the person remove or delete specific electronic communication(s);(b) that the person shares an apology or correction as the court deems appropriate in the circumstances;(c) that the person shall not, for such period as the court may specify, communicate by any means with the other person or that the person shall not approach within such distance as the court shall specify of the place of residence or employment of the other person.

- **PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS (Improper Use) ACT, 2015** (introduced by Minister Pat Rabbitte)
  - Summary: An Act to make it an offence for a person to send, or cause to be sent, by means of a public electronic communications network a message or other matter that is grossly offensive or menacing in character.

Important resources

1. **YouTube: "CEOP Channel"**
   Child Exploitation and Online Protection Centre

2. **www.Nobullying.com**

3. **www.watchyourspace.ie**

4. **www.webopedia.com/quick_ref/textmessageabbreviations.asp**

5. **www.Hotline.ie**

6. **The Garda National Crime Prevention Unit,**
   Garda H.Q., Harcourt Square, Dublin 2.
   Tel: (01) 6663362, Fax: (01) 6663314
   Email: crime_prevention@garda.ie
   www.garda.ie

7. **Office for Internet Safety**
   www.internetsafety.ie

8. **Child Safety Issues**
   www.childline.ie

9. **Website of National Parents Council**
   www.npc.ie

10. **Tips on Internet Safety**
    www.webwise.ie

11. **Irish hotline for public to report child pornography and other illegal content on the internet**
    www.hotline.ie

Send any questions to: **internetsafetytalk@lurtel.ie**

For other products in our range why not visit:

www.schoolswebsites.ie

For any school or other organisation. Simple, user friendly, cost effective websites

www.echipmunk.ie

Online management system for Irish Primary Schools

www.easygrouptexts.com

For clubs and organisations. Send texts and emails to members

www.manageourwater.com

Online management system for Group Water Schemes