

Safe Social Networking

Guidelines for those working with young people



by
Youth Work Ireland



Youth Work Ireland

Youth Work Ireland
20 Lower Dominick Street
Dublin 1

Tel: 01-8729933

Fax: 01-8724183

Email: info@youthworkireland.ie

Website: www.youthworkireland.ie

Contents:

Introduction	5
Acknowledgements	6
Copyright	6
Disclaimer	6
Section 1: Social Networking Safety	7
1.1 What is Social Networking?	8
1.2 General Benefits	9
1.3 General Risks	10
1.4 General Safety Tips	12
1.5 Advice to Young People on Using Social Networking Websites	13
1.6 Tips by Young People for Young People	14
1.7 Reporting a Complaint	17
Section 2: Social Networking - Site By Site Safety	20
Introduction	21
2.1 Bebo	21
2.2 Myspace	24
2.3 YouTube	28
2.4 Facebook	29
2.5 Second Life	31
2.6 Other Sites	35
Section 3: Cyberbullying	36
3.1 What is Cyberbullying?	37
3.2 What Makes Cyberbullying Different	38
3.3 Responding To Risk	38
3.4 Cyberbullying Safety Tips	39
3.5 Tips for Young People	39
3.6 Tips for Parents	40
Section 4: Other Issues	41
Introduction	42
4.1 Instant Messaging	42
4.2 Using Mobile Devices	44
4.3 Online Gambling.....	45
4.4 Use of Credit Cards Online.....	46
4.5 Online Gaming Issues	47
Section 5: Appendices	53
5.1 Acceptable Use Codes & Policies	54
5.1.1 BECTA - Responding to Incidents	54
5.1.2 Sample Acceptable Usage Policy	58
5.2 Resources	62
5.2.1 Irish Contact Agencies	62
5.2.2 Useful Irish Web Based Resource	63
5.3 Relevant Legislation	64
Bibliography of References	65

INTRODUCTION

In 2003 Youth Work Ireland (then the National Youth Federation) developed a set of guidelines and poster campaign on Safe Internet Use for those working with young people called Safe Surfing.

These guidelines focused on general safe use of the Internet and email with a focus on chatrooms, newsgroups, bulletin boards etc and also providing supporting documentation and templates to assist with the provision of Internet access by youth organisations. However, these guidelines pre-dated the explosion in the use of social networking sites such as Bebo, MySpace, YouTube and Facebook necessitating the need to revisit the guidelines and include a section on the safe use of these social networking sites.

Given that these social networking sites have become the biggest single vehicle for young people accessing the Internet it was agreed by the working group tasked with developing this document that there should be a separate set of safe social networking guidelines. These safe social networking guidelines aim to provide an overview of social networking, both the benefits and dangers in relation to their use, how to respond to safety concerns, to outline what the primary social networking sites are and their own safety measures and tips and to specifically look at responding to the issue of cyberbullying. These guidelines are not prescriptive but do aim to provide a grounding in safe practices many of which are repeated across the various well known social networking websites.

The use of the Internet by children and young people is an emotive issue, which has generated much public debate in recent times. However, we live in the era of information technology, where most young people now have access to a computer be it at home, school/college, via mobile phones and increasingly in the high street. We must accept that we cannot prevent young people using the Internet and more specifically social networking sites. Indeed it should be encouraged, as it is potentially a wonderful leisure, educational and developmental tool that can open up many opportunities and new worlds for young people at the touch of a button.

Our role should be to ensure, to the best of our ability, that young people are using and enjoying the Internet in a safe and responsible manner. These guidelines represent in a small way an attempt to assist this process.

These guidelines also make reference to a number of related issues not covered in the original Safe Surfing guidelines but raised by youth workers during the consultation process as needing to be addressed. These include safety when using mobile devices; instant messaging; online gambling; using credit cards online and online gaming.

Finally, it should be noted that the information and supporting templates contained in the original Safe Surfing guidelines remain useful and they have been updated in tandem with the development of these Safe Social Networking guidelines, with both documents being available for youth workers to be downloaded at www.youthworkireland.ie OR www.iywc.com .

ACKNOWLEDGEMENTS

We would like to acknowledge our appreciation to the following in the production of these guidelines:

Drafter & Editor: Fran Bissett, Youth Work Ireland National Office

Design & Layout: Gina Halpin, Irish YouthWork Centre, Youth Work Ireland National Office

Safe Social Networking Guidelines Working Group

Fran Bissett, Youth Work Ireland National Office

Helen Butler, Youth Work Ireland, Galway

Edweena Dully, Midlands Regional Youth Service

Trish Flynn, Clare Youth Service

Bernard Hackett, Waterford Regional Youth Service

Mary Lynch, Youth Work Ireland, Monaghan

Other Contributors

Nora Butler, Kerry Diocesan Youth Service

Mairtín Lane, Kildare Youth Services

Young People from Waterford Regional Youth Service: Peter Coffey, David Roche and Aidan Sinnott

COPYRIGHT REPRODUCTION PERMISSION

Permission is granted to photocopy and/or reproduce the content and/or sections from this publication providing the source is recognised as follows:

Youth Work Ireland, (2009), Safe Social Networking: Guidelines for those Working With Young People, (Dublin: Irish Youth Work Press)

DISCLAIMER

Although every effort has been made to ensure that the information in these guidelines is accurate and up to date at the time of going to print, Youth Work Ireland cannot accept responsibility or liability for any errors or omissions.



SECTION ONE: SOCIAL NETWORKING



1.1 What is Social Networking?

1.2 General Benefits



1.3 General Risks



1.4 General Safety Tips



1.5 Advice to Young People on Using Social
Networking Websites

1.6 Tips by Young People for Young People

1.7 Reporting a Complaint



1.1 WHAT IS SOCIAL NETWORKING

Social networking websites have become a massive online phenomenon and began to be developed in the late 1990s to enable friends to stay in touch with each other. However it is really over the last five years or so that their usage has expanded significantly and their use has been accompanied by much publicity both positive and negative. Social networking sites develop from an initial set of members who send out messages inviting their friends to join the site. New members repeat the process, thus the total number of members and links grow in the network. The value of the network for members is exponentially linked to the number of people in the network. Social networking websites use technology known as web 2.0, which essentially means that the websites are dynamically created by users who upload their own content to make the website what it is.

Social networking sites offer features such as automatic address book updates, viewable profiles, the ability to form new links with other users and other forms of online social connections. These networks tend to be organised around shared common interests. MySpace, for example, has built itself around music and party scenes.

Of particular interest within these guidelines will be Bebo, which is an online community where friends can post pictures, write blogs and send messages to one another. Each member has their own personal page, on which they can tell the world about their likes and dislikes, link with friends and post up photos of their lives. Bebo also links people together through schools and colleges and it is the social networking site most used by young people in Ireland and per head of population used by more by young people than in any other country in the EU.

Bebo more so than other social networking sites has become a personalised space for a young person where they can present themselves in a way that they can control. Danah Boyd, one of the world's leading authorities on social networking software recently observed in explaining the attraction of these sites to young people:

“Most of their [teenagers] space is controlled space. Adults with authority control the home, the school, and most activity spaces. Teens are told where to be, what to do and how to do it. Because teens feel a lack of control at home, many don't see it as their private space”

1.2 GENERAL BENEFITS

There are a number of significant benefits to using social networking sites some of which are outlined below:

Creating Their Profile

Once registered with a particular social networking website, users can post a profile of themselves which can be read by others online. The goal is to look popular or 'cool' and to be acknowledged by their peers as being popular or 'cool' and someone you would like to have as an online friend. The number of page views on a users profile is a proxy indicator of how popular they are. For users the more views the better.

Adding Links to Friends Profiles

The next step is to invite their existing contacts to join their profile. They are usually invited from their existing e-mail and messenger contact lists.

Creating Blogs and Posting Comments

An explicit reaction to their online presence offers valuable feedback to teenagers as they strive to create their identity. Comments are also a sign of affection and affiliation. There is a definite social etiquette at play; comments are expected to be reciprocated.

Privacy

Many young people are using social networking sites everyday; it's just another part of their life. They can be surfing social networking sites while doing their homework, downloading music, or chatting on Instant Messenger. They want to be with their friends in a space that is not inhabited by adults and because of the constraints imposed on them; they rarely get the opportunity to do this outside their virtual environment.

Experimentation

Sites like Bebo allow young people to experiment in reasonable safety with versions of who they are. They try out various presentations of themselves, get feedback from friends and peers and work on ideas about music, fashion and their other interests in order to better represent the person they want to be.

There are potential risks to using social networking sites such as Bebo which are well publicised, which most young people are aware of and yet they still come in their thousands to these sites. For young people the benefits and positives far outweigh these risks. It is important to recognise when working with young people on their use of social networking and not to approach it with a negative mindset as merely a problem to be dealt with.

1.3 GENERAL RISKS

Risks of Using Social Networking Websites

Like most online activity there are risks to the users. In the case of social networking websites the primary risks involve the unintentional disclosure of personal information, bullying or harassment (cyberbullying), and in a small number of cases targeting of users by predators.

It is important to highlight that young people may not only be vulnerable to these activities but they may on occasion also be involved in initiating, maintaining or perpetrating the same against other, young people, adults and /or organisations.

Disclosing Personal Information

The way these sites work is based on users creating sites /profiles including their personal opinions and in most cases photographs on aspects of their lives. This enables people with the same interests to meet others. Users' profiles are also a way of attracting potential girlfriends or boyfriends. Many young people will send flirtatious comments to others having been attracted to photos on their site.

The problem with posting personal information to the Internet is that as soon as it goes online, the user has lost control over who will see it and how it will be used. Pictures can be easily be copied and displayed in a completely different context.

Given that most photos now are digitally produced, they can be even be altered or distorted. Many social networking websites give the impression to users that they are in closed networks of friends. This encourages young people to disclose more personal information or to be more intimate with their communications than they would be if they thought it was a completely public forum.

The fact that certain websites claim to connect students from the same school does not necessarily mean that they are safer. The information provided by users when they are registering is often not validated. Any individual can create a user profile pretending to be anyone else. Moreover, anyone regardless of their real or pretend age can join any online community they choose irrespective of their age just as the can when joining a chatroom or bulletin board online.

Bullying and Harassment

Many social networking sites include a facility where users are encouraged to rate profiles they come across on the site. This relatively innocuous capability can lead to users being sent harmful comments. As these comments usually relate to personal pictures posted on the websites they can often relate to the person's physical appearance, ethnicity, race etc.

There is also a tendency for offline bullying to be amplified online. The perception exists that there is a reduced likelihood of being caught because they are not directly confronted by the consequences of their bullying. Therefore, it is easier for young people to engage in bullying online than it is in the offline world. Young people need to be made aware that despite this perception it is relatively easy to trace online bullies and that the consequences of being identified can be very severe. Many online bullying activities are illegal and can end up being dealt with by the police.

Cyberbullying is cover in more detail in Section three.

Being Targeted by Predators

Because there is no routine validation of users, personal information contained in profiles can be used by unscrupulous individuals as the basis for scams, malicious attacks, or in the worst cases by paedophiles to groom potential victims. These people often operate by collecting small pieces of information at a time while slowly building up a bigger picture of their target without arousing suspicion. They can use multiple different identities to avoid detection.

Employment Prospects

An individual profile/page on a social networking site can be used (and increasingly is) by employers and prospective employers to check what type of activities an individual is engaged in away from work which may then be used to assess their character or suitability for a job/promotion. It can also be used to check whether someone who has taken sick or compassionate leave or called in sick on a particular day is telling the truth or not..

So it is important for people to be circumspect in terms of what personal information or information on their leisure pursuits/activities they disclose on social networking sites and importantly what other people with access to their profile say about them on their profile page. There is ample evidence of individuals being dismissed from employment on the basis of information their employer has acquired on them from social networking sites.

1.4 GENERAL SAFETY TIPS

Advice to Parents

As with all other Internet safety issues the single biggest positive impact on young people's online behaviour is caused by an active engagement by parents in their online life. Remember the chances of a young person sharing their online experiences with you will be greatly reduced if they think that telling you about a problem will result in them being banned from using the Internet.

The More You Know, the More You Can Support.

Get your young people to talk about what they use the technology for – whether it is a mobile phone, a PC or a video games console. Young people will enjoy the fact that they can teach you something and it is an opportunity to share activities with them.

Encourage Your Young Person to be Careful When Disclosing Personal Information.

Being conscious of when and where it is all right to reveal personal information is vital, it is especially important when using social networking sites. A simple rule could be that a young person should not give out any information or pictures that they wouldn't be prepared to print on a t-shirt and wear into town.

Encourage Respect for Others.

As in everyday life, there are informal ethical rules for how to behave when relating to other people on the Internet. These include being polite, using correct language and not harassing others. Make young people aware that despite the perceptions to the contrary, online bullying is easier to detect and trace than offline bullying. Online bullying can have more severe consequences for the victim because it is so difficult to escape from. Also because of the code of practice adopted by Internet Service Providers and mobile phone operators, companies are obliged to involve the Gardaí when illegal activity is reported to them.

Know Your Young Person's Net Use.

To be able to guide your young person with regard to Internet use, it is important to understand how young people use the Internet and know what they like to do on-line. Let your young person show you which websites they like visiting and what they do there. Acquiring technical knowledge could also make it easier to make the right decisions regarding a young person's Internet use.

1.5 ADVICE TO YOUNG PEOPLE ON USING SOCIAL NETWORKING WEBSITES

Do know who can access your personal information – many sites allow you to decide which parts of your profile can be accessed by others. Assume that everything is public unless you are sure that it isn't. Opting for private doesn't always mean that only your friends can see your profile. In some cases it means that everything you put on your profile can be seen by everyone but only your friends can post comments or IM you.

Do trust your instincts - If it doesn't look or "feel right", it probably isn't. If you find something online that you don't like or makes you feel uncomfortable, turn off the computer and tell an adult.

Do be careful with your personal information - The problem with posting personal information to the Internet is that as soon as it goes online, you have lost control over who will see it and how it will be used. Pictures can easily be copied and shared with 100,000 of others at the press of a button. Because of the digital nature of the photos, they can even be altered or distorted. Don't post any pictures that you wouldn't want everyone you know to see, that includes your parents, teachers or youth workers.

Don't assume everyone you meet online is who they appear to be - The fact that certain websites claim to connect students from the same school means nothing. The information provided by users when they are registering is not checked. Anyone can create a user profile pretending to be anyone else. Moreover, anyone regardless of their real or pretend age can join as many as they want.

Don't post information that could be used to find you offline – without meaning to; you can give away information that could help someone to find you. Be careful of posting photos with things like car registration plates or identifiable landmarks in them. Avoid posting messages to blogs along the lines of "I usually walk home down the lane by the railway tracks". There are some people out there who will piece together little snippets of information about you over a long period of time.

Don't reply to messages that harass you or make you feel uncomfortable! - Even though you may really want to, this is exactly what cyberbullies want. They want to know that they've got you worried and upset. They are trying to mess with your head. They want to think that they are important by being able to get a reaction from you. Don't give them the pleasure.

Source: www.webwise.ie

1.6 TIPS BY YOUNG PEOPLE FOR YOUNG PEOPLE

This section was developed by young people working in Waterford Regional Youth Service who took a look at Facebook, Bebo and Myspace and condensed the safety information from each into one, to minimise the overlap and in a way that made sense to them.

The problems encountered in social networking or other anonymous online communities typically fall into three categories:

- ID theft, fraud and privacy abuse;
- Cyber bullying, cyber stalking and harassment
- Sexual predators, con artists and sexual exploitation.

Here are a few safety tips that should help you stay safe online

Keep Your Personal Information To Yourself

Never divulge any personal information that could be used to find or identify you in real life in a public forum. Password protect this information. This information includes your real name, address, telephone number, mobile number or links to websites or other profiles that might give this information away. It also includes this kind of information about your friends and family. Your personal information could be easily abused and misused. Your password can often be guessed, your identity can be stolen, it can be used by people wanting to defraud you or groom a teen into an offline meeting, or used to cyberstalk or harass you or by cyberbullies. It's your personal information...PROTECT IT!

Protect Your Password!

Keep your password to yourself and don't pick one that's easy to guess. (Keeping it on a post-it note glued to your monitor may not be the best way of storing your password securely.)

Don't Forget That Your Profile Is A Public Space

Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screens name, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school.

Are You Really Willing To Let Your Boss or Parents Read Your Profile

Don't post anything in public that you don't want your parents, principal, boss, university president or boyfriend or girlfriend to see. These posts tend to last longer than any of us thought they could. They are passed around and discoverable by search engines. You are never truly private when online. Remember that. Password protect everything and guard your password.

People Aren't Always Who They Say They Are. Be Careful About Adding Strangers To Your Friends List.

It's fun to connect with new friends from all over the world, but avoid meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.

Think about keeping some control over the information you post. Consider restricting access to your page to a select group of people, for example, your friends from school, your club, your team, your community groups, or your family.

Make sure your screen name doesn't say too much about you. Don't use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.

Consider not posting your photo. It can be altered and broadcast in ways you may not be happy about. If you do post one, ask yourself whether it's one your mum would display in the living room.

Be wary if a new online friend wants to meet you in person. Before you decide to meet someone, do your research: Ask whether any of your friends know the person, and see what background you can dig up through online search engines. If you decide to meet them, be smart about it: Meet in a public place, during the day, with friends you trust. Tell an adult or a responsible sibling where you're going, and when you expect to be back.

ThinkB4UClick

Before posting something online, check and make sure it says what you wanted it to say, can't be misconstrued and is being posted at the right place or sent to the right person. Think about the person on the other side. Many cyberwars start with a careless message.

Take5!

If something upsets you online, put down the mouse and walk away from the computer...so no one will get hurt! Take five minutes to do something you enjoy doing for five minutes to help you calm down and reply with a clear head.

They are Just People You Meet Online, Not Real Friends

Remember that your online friends are not really your friends. You may like them, think they understand the real you and even connect. But, unless you know them offline, they are not real friends. They are just cyberfriends. People who are smarter than you have been tricked. Don't become a victim!

I'm Receiving Unwanted Messages. What should I do?

There are a few things you can do:

- You can anonymously report messages by clicking on the "Report Message" link under the name and picture of the sender when viewing a message.
- You can easily block any user on social networking sites from seeing or contacting you by entering their name in the Block People section on the Privacy page.
- You can limit the people who can find you in searches, which in turn limits who can message you. Or you can block certain users.

Don't Be An Easy Mark

If something seems too good to be true, it's not true. Period. No exceptions. Does it make sense to you that the brother-in-law of the former Nigerian president found you out of the 700 million other users online to entrust with their 500 million Euro?

Harassment, Hate Speech and Inappropriate Content Should Be Reported

If you feel someone's behaviour is inappropriate, react. Talk with a trusted adult, or report it to the website or the authorities.

Trust your gut feeling if you have suspicions. If you feel threatened by someone or uncomfortable because of something online, tell an adult you trust and report it to the police and the social networking site. You could end up preventing someone else from becoming a victim.

Tell a Trusted Adult and Report Cybercrime

If you are a minor (under 18 years of age), make sure that you tell your parents or another trusted adult if something goes wrong. Don't try and handle it yourself. If it involves dangerous or criminal activity, or someone you suspect is a predator or criminal, report it to your local law enforcement office.

Sources: www.facebook.com www.bebo.com www.youtube.com

1.7 REPORTING A COMPLAINT



Office for Internet Safety

The Office for Internet Safety is an Executive Office of the Department of Justice, Equality & Law Reform. The Office for Internet Safety has been established by the Government to take a lead responsibility for Internet safety in Ireland, particularly as it relates to children. The Office for Internet Safety aims to build linkages and cohesion between all Departments and agencies to ensure that the State provides the best possible protection for the community and promotes internet safety, particularly in relation to combating child pornography.

The Office for Internet Safety will build on and oversee the current self-regulatory framework which is in place under the **Internet Service Providers Association of Ireland (ISPAI)**. Central to their relationship with ISPAI is an agreement to subscribe to a code of ethics and practice for the industry. As part of this agreement the industry supports **www.hotline.ie** which receives and processes reports of child pornography and other inappropriate Internet content.



www.hotline.ie

The **www.hotline.ie** service provides an anonymous facility for the public to report suspected illegal content encountered on the Internet, in a secure and confidential way. The primary focus of the Hotline is to combat child pornography. However, other forms of illegal content and activities that exist on the Internet can be reported using this service.

The Hotline, run by the Internet Service Providers Association of Ireland (ISPAI) since November 1999, is part financed by the European Commission's Safer Internet Plus Programme. It is supervised by the Department of Justice, Office for Internet Safety (OIS), in cooperation with An Garda Síochána and is a member of **INHOPE**, the International Network of Hotlines.



The **www.hotline.ie** service exists to combat illegal material on the Internet. All reports are assessed and where content is found to be illegal action is taken.

Members of the public can report content they suspect to be illegal when using any of the following services:

- Websites (including sites for mobile WAP or equivalent)
- Unsolicited email (spam advertising illegal content)
- Peer-to-peer file sharing networks
- Online forums, bulletin boards, blogs, *social networking sites
- Newsgroups
- Online chat rooms or instant messaging

** Reporting complaint mechanism in relation to particular networking sites is dealt within the next section.*

If an individual is not sure if the material is illegal or not, it does not matter, report it to the Hotline and it will be assessed. Types of illegal content that should be reported are:

- Child pornography
- Child grooming activities
- Child sex tourism

- Child trafficking
- Racism and xenophobia
- Incitement to hatred
- Financial scams (usually sent by spam)
- Other content (used to submit a query to the Hotline or notify about content not in above categories).

Making a Report/Complaint

Upon entering the www.hotline.ie site there is a large **Click to Report** icon on the top right hand side of the page and this option is there on any page within the site that is visited. Clicking on this icon takes the user into a reporting template. The reporting template is straightforward and easy to complete and asks for the following:

- Identify where the source of the complaint is
- A description of the complaint
- What is suspicious about the content (based on the above headings)
- An option to leave contact details or make the complaint anonymous

How the Hotline Processes a Report and the Information Provided Within It

The Hotline's operational process starts when a report is received from the public or from another international hotline. The submissions are generated through electronic forms that are available on www.hotline.ie and reports can be submitted completely anonymously.

When a report is received, the Hotline will send an acknowledgement where contact information has been given. The preference is to provide this reply by e-mail. The content of the report is then transferred to the Hotline operational Database, which is held in encrypted form for added security.

Under the legal system in Ireland, only a court of law can determine that a criminal offence has been committed and that material (i.e. child pornography) relating to that offence is actually illegal. Therefore, the Hotline can only determine that something is "probably illegal" with reference to the criteria given in the relevant Irish law. In the case of Child Pornography, for example, that is the **Child Trafficking and Pornography Act (1998)**.

Once the report has been logged, a trained Hotline Analyst will try to find the material on the Internet. If the subject content to which the report refers is found, it will then be assessed as to whether it is probably illegal under Irish law. If it is not illegal, no further investigatory action is taken. If the content is considered to be probably illegal under the relevant Act, the next step is to determine the location of the material as accurately as possible.

The Hotline staff use a suite of tools and their experience to attempt to trace and locate the source, be it a web host server, a peering node (P2P), an e-mail server or other Internet based service. If the reported material is traced to a server located in Ireland, or is found to have originated from an Internet user account provided by an Irish ISP, the ISP of that customer is identified.

The Hotline then issues notification to An Garda Síochána and simultaneously a "take down" notice is issued to the ISP, where they are a member of the ISPAI. The ISP is responsible for the timely removal of the specified probably illegal content from their servers to ensure that other Internet users cannot access the material. The decision to initiate a criminal investigation is a matter for An Garda Síochána.

If the content source is traced to another country, there are two possible actions. If an INHOPE hotline exists in that country, then details based on the original report, including the Hotline's findings, are forwarded to the other hotline for processing. If the material is located in a country having no INHOPE presence, the Hotline will attempt to have action taken by providing details to An Garda Síochána for transmission to the source country through international law enforcement channels.

In all the above cases, even if the person reporting has provided contact details, these are not provided to other parties. Only the details of the suspected content and the technical findings of the Hotline are transmitted.

Once this notification procedure is completed, the Hotline records the action that was taken in the database and closes the report.

Further Resources

The Office for Internet Safety produces occasional publications to advise and examine the role of the ISP in Ireland. The following is list of their more recent publications which can all be downloaded free from the website (www.internetsafety.ie)

A guide to cyberbullying

Get With IT! Leaflet - Internet Safety for Parents

Get With IT - A parents guide to social networking websites

Get with IT - A parents guide to filtering technologies

Get with IT - A parents guide to new media technologies

Contact Details:

Office for Internet Safety

Floor 3, Block 2, Harcourt Centre

Harcourt Street

Dublin 2

Tel: 01 408 6122 Fax: 0 4086142

Email: internetsafety@justice.ie

Web: www.internetsafety.ie

ISPAI www.hotline.ie Service

Unit 24 Sandyford Office Park

Dublin 18

Tel: 1890 610710 Fax: 01 294 5282

Email: info@hotline.ie

Web: www.hotline.ie

SECTION TWO: SOCIAL NETWORKING - SITE BY SITE SAFETY

Introduction

2.1 Bebo

2.2 Myspace

2.3 YouTube

2.4 Facebook

2.5 Second Life

2.6 Other Sites



INTRODUCTION

This section looks specifically at number of the most used social networking websites, namely Bebo, MySpace, YouTube Facebook and Second Life. The section briefly outlines what each site is and includes sections of their own safety advice and mechanisms for reporting complaints. This is not a comprehensive list of social networking sites just those that people may be most familiar with. There are a number of other sites which are referenced which at the end of this section.

2.1 Bebo



What is Bebo?

Bebo is an online community where members can stay in touch with their friends, connect with friends, share photos, discover new interests and just hang out online. Each member has their own personal page, on which they can tell the world about their likes and dislikes, link with friends and post up photos of their lives.

It is hugely popular with children and young people in Ireland, being the third most popular website in Ireland (after Google.ie and Google.com). 10% of its total users are Irish, as compared to 11% from the US for example. The reason for such high usage is that it was the first social networking site to integrate with Irish schools. On the plus side with regard to safety, at the time of print, Ireland was currently the only country in Europe to have Internet safety integrated into the classroom environment through the Social, Personal and Health Programme at Junior Certificate Level.

General Safety

The first thing you should do if you are having issues with content on the Bebo website is report the matter to the website owners. Once you have informed them of the existence of harmful content on their site they are obliged to remove it within a reasonable amount of time.

Youth workers who have concerns about content on the site can use the on-line Bebo reporting tool. Click on the **'Report Abuse'** link on the individual's homepage.

If you are not a member of the Bebo website you can report abuses on the bebo site by submitting your issues through the **Contact Us form** on the site

In all cases when reporting abuse, Bebo will need any of the following details that apply to what is being reported so that they can identify the content concerned:

- Username or member ID #
- Email address
- Name of the School (if it is a school site)
- The exact content location (name of the photo, club, poll, forum, or quiz).

Some Bebo Safety Tips

Minimum Age at Bebo: Bebo sets the minimum age of their users at 13. They mean it. While they can't know anyone's real age, if an underage user is reported to them and Bebo can confirm from statements on their profile page that the user is underage, they will be notified. Unless they can prove that they are 13 their profile page will be deleted.

Keep Your Personal Information to Yourself: Never divulge any personal information that could be used to find or identify you in real life in a public forum. Password protect this information. This information includes your real name, address, telephone number, mobile number, your workplace if applicable, health club, or links to websites or other profiles that might give this information away. It also includes this kind of information about your friends and family. You may be sharing more information than you intended to by including a photo with something showing in the photo that can identify you, your family or further details about yourself. Your personal information could be easily abused and misused. Your password can often be guessed, your identity can be stolen, It's your personal information...PROTECT IT!

They are Just People You Meet Online, Not Real Friends: Remember that your online friends are not really your friends. You may like them, think they understand the real you and even connect. But, unless you know them offline, they are not real friends. They are just cyberfriends. You don't know if that cute twenty-year old guy is cute, twenty or even a guy. Treat them like strangers you encounter on a bus. Chat with them, but don't spill your guts to them. They should not be entrusted to provide you with advice about important life issues, or confided in, no matter how tempting it may be. No matter how often you have chatted with someone or how much you think you know about them, you never really know who you are chatting with online. People who are smarter than you have been tricked. Don't become a victim!

Protect Your Email Address: Use a free e-mail service, such as yahoo or hotmail. That way if things go wrong, you can just delete that account and you do not put your own/personal email address at risk. Also, get a good SPAM blocker programme and never reply to a SPAM message that asks you to be removed from their lists. This will identify you as someone who reads the SPAM and will encourage more and more SPAM.

Are You Really Willing to Let Your Boss or Parents Read Your Profile: Don't post anything in public that you don't want your parents, boss, teacher/youth worker, partner boyfriend/girlfriend to see. These posts can be passed around and can be discovered by using standard search engines. You are never truly private when online. Remember to password protect everything and guard your password.

Protect your computer: Make sure you have a good firewall/automatically updated anti-virus software installed on your computer. You should also get a good spyware or adware blocker too. Be careful about downloading or opening files sent to you, even from people you know. Many viruses masquerade as someone you know. Hacking tools and programmes (such as Trojan horses) can give someone a backdoor to your computer, all your passwords and banking information.

Protect Your Password! Keep your password to yourself and don't choose one that is easy to guess. Keeping it on a post-it note glued to your monitor at work or at home is common but is clearly not good for storing your password securely. To protect yourself, come up with a secret code word to use with friends online. If you are chatting with someone and suspect that it may not be genuine, ask them for the code word. If they don't know it, report it and then log-off immediately. Be aware also that the people who abuse your password the most are often your close friends. So make sure you do not share your password with anyone.

Get a Life! Bebo wants you to spend lots of time enjoying their site. But even they agree with me that sometimes everyone can spend too much time online. Make sure that you don't spend all of your time online. Don't give up on your offline friends, activities or social life. I know that we are all thinner, cuter, more popular and smarter online than we are in real life. : But spending less time online has its benefits too. (We may actually become thinner, cuter, more popular and smarter in RL. :))

Don't be an easy target. Do not be taken in by offers that appear to be too good to be true because are. No exceptions.

ThinkB4UClick: Before posting something online, check and make sure it says what you wanted it to say, can't be misunderstood and is being posted at the right place or sent to the right person. Think about the person/people on the other side. Many cyberwars start with a careless message.

Don't fall for a "phishing" scheme: Phishing is when an ID thief sends millions of e-mails or Instant Messages pretending to be your bank, or online service, like Paypal. They look real and try to trick you into responding quickly without thinking. They will claim that someone has broken into your account, or that changes were made to your account or need to be made to your account. They ask you to log in using the link in the e-mail. The link takes you to their site, but you think you're at your bank's site. You type in your login and password. A page pops up telling you that your account is secure and thanking you. Your real account is accessed and emptied within minutes. If you aren't sure if the e-mail is real or not, check with the site directly by typing it into your browser. If you were already caught by a "phish" report it to your bank or the website right away.

Take5! If something upsets you online, put down the mouse and walk away from the computer for a while. Take five minutes to do something else to help you calm down and reply with a clear head. If you find a post that is designed to harass, cyberbully, threaten or frighten you or someone else, click on 'Report Abuse' on the offenders profile. It violates Bebo's terms of service and will be addressed by their abuse team.

Let Bebo know if there is a problem: Bebo doesn't permit anything that hurts their members. Check out their terms of service and report abuses by clicking on the 'Report Abuse' link on the offenders' profile. If conditions of use are violated they can and do delete people user's profiles.

Tell an Adult and Report a Crime: If you are a minor (under 18 years of age), make sure that you tell your parents or another trusted adult if something goes wrong. Don't try and handle it yourself. If it involves dangerous or criminal activity, or someone you suspect is a predator or criminal, it may need to be reported to the Gardai. Bring them a printout, but also make sure it isn't deleted. The police need the original communication to have the acquired information necessary to trace the communication and who sent it.

Webwise Advice on Bebo

If you are a teacher or ICT Coordinator and are aware of a website which may need to be blocked or re-categorised, contact the NCTE Broadband Service Desk.

If you have a serious concern that content /misuse encountered on the Internet may be illegal, you should report it to www.hotline.ie. The www.hotline.ie service was established in November 1999 to combat illegal young person pornography on the Internet. (for more detail, see Section 1.6 Reporting a Complaint)

The service provides a secure and confidential environment where you may anonymously report such content if you encounter it on the Internet. Whilst the primary focus of the Hotline remains child pornography, other forms of illegal material do exist on the Internet (such as racist material, incitement to violence against individuals, etc.) and these may be reported using the Hotline service. To report suspected illegal content / misuse, use the on-line form on www.hotline.ie .

Source: www.webwise.ie

2.2 MYSPACE



What is MySpace?

MySpace is an online community that lets you meet your friends' friends. MySpace makes it easy to express yourself, connect with friends and make new ones, but who you let into your space, how you interact with them, and how you present yourself online are important things to think about when using any social networking site and Myspace is no different.

General Safety

Below are some common sense guidelines that MySpace itself recommends that you follow when using MySpace:

- Don't forget that your profile and MySpace forums are public spaces. Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screen names, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day or a picture of you in front of your office or school.
- People aren't always who they say they are. Be careful about adding strangers to your friends list. It's fun to connect with new MySpace friends from all over the world, but avoid meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.
- Harassment, hate speech and inappropriate content should be reported. If you feel someone's behavior is inappropriate, react. Report it to MySpace or the authorities.
- Don't post anything that would embarrass you later. It's easy to think that only our friends are looking at our MySpace page, but the truth is that everyone can see it.
- Think twice before posting a photo or information you wouldn't want your parents, potential employers, colleges or boss to see!
- Don't say you're over 18 if you're not. Don't say you're younger than 18 if you're not. If MySpace customer service determines you are under 14 and pretend to be older, we will delete your profile. If customer service determines you are over 18 and pretend to be a teenager to contact underage users, we will delete your profile.

MySpace Tips for Teens

- Don't say you're older than you are. MySpace members must be 14 years of age or older. We take extra precautions to protect our younger members and we are not able to do so if you do not identify yourself as such. If MySpace customer service determines you are under 14 and pretend to be older, we will delete your profile.
- MySpace is a public space. Members shouldn't post anything they wouldn't want the world to know (e.g., phone number, address, IM screen name, or specific whereabouts). Don't post anything that would make it easy for a stranger to find you, such as your local hang out. It's always fun to post pictures but remember that what you might consider a harmless picture of you and your friends in your uniforms at a school football game, is actually a map telling a stranger exactly where you go to school.

- Don't post anything that could embarrass you later or expose you to danger. Please remember that MySpace is public and many people have access to what you post, including potential employers, colleges, your teachers and peers at school that you might not even know. You shouldn't post photos or info you wouldn't want adults to see or people to know about you.
- Protect your privacy. Set your profile to private which lets only your friends view your profile. Users under the age of 16 are automatically assigned a private profile. Only accept friend invitations from people you know and trust.
- People aren't always who they say they are. Be careful about adding strangers to your friends list. It's fun to connect with new MySpace friends from all over the world, but avoid meeting people in person whom you do not fully know. Remember that you don't really know who is on the other end of an Internet connection.
- Harassment, hate speech and inappropriate content should be reported. If you encounter inappropriate behavior, inform your parents or a trusted adult and report it to MySpace or the authorities.
- Don't get hooked by a phishing scam. Phishing is a method used by fraudsters to try to get your personal information, such as your username and password, by pretending to be a site you trust. If you suddenly start receiving abnormal bulletins or messages from a friend, they might have been phished. Check with them before opening any files or clicking on any links. If you think you, or a friend, are a victim of phishing, change your password immediately.
- Avoid in-person meetings. Don't get together in person with someone you "meet" online unless you are certain of their actual identity. Talk it over with an adult first.
- Although it's still not risk-free, arrange any meetings in a public place and bring along friends, your parents, or a trusted adult.
- Think before you post. What's uploaded to the net can be downloaded by anyone and passed around or posted online pretty much forever. You shouldn't post photos or info you wouldn't want adults to see or people to know about you.

MySpace Tips for Parents

Start a Conversation

Talk to young people you work with about why they use MySpace, how they communicate with others, and how they represent themselves online. Recognize the importance of social networking in their daily lives, similar to that of cell phones, email or instant messenger, and express an interest in understanding the role it plays.

Ask them why they like being online and who they hang out with online. Ask them to show you their friends, what they are listening to, and what interests them within the community.

Report Inappropriate Behavior

Harassment, hate speech, and inappropriate content all violate the MySpace Terms of Use and should be reported. If your kids encounter inappropriate behavior, they should report it to you, the authorities and/or MySpace, as the situation merits. To report a problem, go to Contact MySpace and select "Reporting Abuse."

Talk About MySpace and the Internet

MySpace, like the rest of the online world, is a public space. Members shouldn't post anything they wouldn't want the world to know (e.g., phone number, address, IM screen name, or specific whereabouts). Tell your teens they should avoid posting anything that would make it easy for a stranger to find them, such as their local hangouts.

Remind them not to post anything that could embarrass them in the future or expose them to danger. Although MySpace is public, teens sometimes forget that the information and photos they post are accessible to others.

Remind Teens to Be Cautious

Just as in the offline world, people aren't always who they say they are. Remind your teens to be careful about adding strangers to their friends list. It's fun to connect with new MySpace friends from all over the world, but members should be cautious when communicating with people they don't know.

Encourage teens to be themselves, but to exercise the same basic safety principles they do in the physical world. They wouldn't chat with a stranger at the mall or give someone they don't know their cell phone number. Remind them that reckless online behavior can be just as dangerous.

They should talk to you if they want to meet an online friend in person, and if you think its safe, any meeting should take place in public, with friends or a trusted adult present.

Safety Settings

MySpace has developed a number of safety features and settings to protect users from unwanted contact and allow control over the privacy of personal profiles, including:

Private Profiles

Every profile has the option of being 'private.' This means that only you and those you have added and approved as friends can see the details of your profile, including your blog, photos, interests, etc.

- To set your profile to 'private,' first sign in to your MySpace account.
- In the 'Classic View of the profile', click on the 'Account Settings' link next to your profile picture
- In the 'New Home Skin' view of the profile, click on 'Settings' from the Control Panel located below your profile picture
- Select 'Privacy' from the top navigation bar
- In 'Online Now' un-select 'Show People When I'm Online'
- Now, scroll to the bottom of the page and click on 'Change Settings' to ensure your setting has been saved.

Pre-approve Comments

The default setting for comments on MySpace profiles does not require comments to be approved prior to appearing on your profile.

- To change your settings so you can approve comments before they are posted, sign in to your MySpace account.
- In the 'Classic View of the profile', click on the 'Account Settings' link next to your profile picture.

- In the 'New Home Skin' view of the profile, click on 'Settings' from the Control Panel located below your profile picture.
- Select 'Spam' from the top navigation bar.
- In 'Comments' select 'Require approval before comments are posted'.
- Now, scroll to the bottom of the page and click on 'Save All Changes' to ensure your updated settings have been saved.

Block Another User

If a user that you do not know or want to interact with contacts you, you have the ability to block them from future contact. Also, if you feel this person may be a threat to yourself or others, immediately notify a trusted adult or law enforcement and report the user to MySpace through the 'Contact MySpace' link at the bottom of every page.

- To block a user from contacting you, go to the user's page and under their profile picture click on the 'Block User' link
- A pop-up window will appear asking you if you are sure you want to block this user
- Click 'Ok.' to confirm.

Turn off the 'online now' status icon

Don't want people to know when you're on MySpace? Turn off the 'online now' status icon so other users can't see when you're on the site and when you're not.

- To conceal your 'online now' status, sign in to your MySpace account
- In the 'Classic View of the profile', click on the 'Account Settings' link next to your profile picture
- In the 'New Home Skin' view of the profile, click on 'Settings' from the Control Panel located below your profile picture
- Select 'Privacy' from the top navigation bar
- In 'Online Now' un-select 'Show People When I'm Online'
- Now, scroll to the bottom of the page and click on 'Change Settings' to ensure your setting has been saved.

Source: www.myspace.com

2.3 YOUTUBE: A WORD ON SAFETY



What is YouTube?

YouTube is a free video sharing website that lets registered users upload and share video clips online at the YouTube.com website. To only view videos you are not required to register. It was launched in 2005 by former PayPal employees and the site was acquired by Google Inc. in October 2006. YouTube is not for young people under the age of 13.

General Safety

In December, 2008, YouTube launched its *Abuse and Safety Center*, providing safety tips to help users deal with issues like cyberbullying, online harassment, and hateful content which is well worth checking out. Listed below are some of the key safety tips that YouTube recommend to their users.

Some Things Are Better Left Private

Posting videos of yourself, your friends or your family can be fun and exciting. You never know who will find it—it might even get featured on the front page, or end up as one of the Most Viewed videos! If your video is personal, consider marking it private so that only your friends and those you share it with can view it.

Protect Your Secret Identity!

If you do post public videos, make sure there isn't anything in them that could help a stranger figure out who you are or where you live. Personal information like your telephone number or home address should NEVER be shared with other users.

Watch out for things like number plates on cars or images of the outside of your house which might accidentally appear in the background of a video and help a stranger to track you down.

Remember, YouTube employees will never ask you for your password, email address or other account information. Don't be fooled if someone contacts you pretending to be from YouTube!

Keep Your Cool, Keep YouTube Safe

Whether it's a flame war, cyber bullying or people just being mean, comments can get nasty sometimes. When you post a video you can choose whether you want to let people comment on your videos at all. If someone leaves a comment on your video that is rude or bothers you, you can always delete the comment. Alternatively, you can select the "comments with approval" option when you upload a video. This means that you get to approve or remove people's comments before they appear on the site.

YouTube doesn't allow videos with nudity, graphic violence or hate. If you come across a video like this, click the link on the video to flag it as inappropriate and submit the form on the next page to report it to YouTube.

YouTube has literally MILLIONS of viewers every day and just like in the real world, most of the people are good, but some aren't. So please take care to protect yourself and your fellow users by keeping personal videos private, your identity a secret, your comments clean and by using the flagging system to report abuse

Source: www.youtube.com

2.4 FACEBOOK



What is Facebook?

Facebook is a social utility that connects people with friends and others who work, study and live around them. People use Facebook to keep up with friends, to share links, to share photos and videos of themselves and their friends, and to learn more about the people they meet. Facebook operates the following Code of Conduct which users are expected to adhere to:

Content Code of Conduct

We want Facebook to be a place where people respect the rights and feelings of others, including third party intellectual property rights. Therefore, we have established certain rules for using Facebook and for posting messages, photos, video and other content (“Content”) on Facebook, which rules are set forth in our **Terms of Use** and in this User Code of Conduct. WHEN YOU USE FACEBOOK, YOU ARE AGREEING TO ABIDE BY THE USER CODE OF CONDUCT AND THE OTHER RULES SET FORTH IN OUR TERMS OF USE. FAILURE TO ADHERE TO THIS CODE OF CONDUCT AND THE TERMS OF USE MAY RESULT, AMONG OTHER THINGS, IN TERMINATION OF YOUR ACCOUNT AND THE DELETION OF CONTENT THAT YOU HAVE POSTED ON FACEBOOK, WITH OR WITHOUT NOTICE, AS DETERMINED BY FACEBOOK IN ITS SOLE DISCRETION. Please refer to our **Terms of Use** for more information about the rules applicable to your use of Facebook and the other rights and remedies of Facebook.

Third Party Content

Facebook allows you to upload and share user generated Content with your friends, such as photographs and videos you upload from your camera, webcam or mobile phone. This means that you may post and share original photographs and video that are of a personal nature that: (i) are of you or your friends, (ii) are taken by you or your friends or (iii) are original art or animation created by you or your friends. It is not intended as a place for you to post third-party copyrighted content, such as the latest episode of a popular TV show or your favorite music video. In addition, we expect our users to use good judgment and respect the copyrights and other intellectual property rights of others. Therefore, in using Facebook, you may not:

- Upload or share any photographs, videos or other Content other than original works that are created by you or another user.
- Post or share any Content that infringes upon or violates the copyright, trademarks or other rights of any third party.
- Attempt to circumvent any content filtering techniques we may employ.
- Inappropriate content.
- While we believe users should be able to express themselves and their point of view, certain kinds of speech simply do not belong in a community like Facebook. Therefore, you may not post or share. Content that:
 - Is obscene, pornographic or sexually explicit.
 - Depicts graphic or gratuitous violence makes threats of any kind or that intimidates, harasses, or bullies anyone;
 - Is derogatory, demeaning, malicious, defamatory, abusive, offensive or hateful.

Unlawful or Harmful Content or Conduct

Although as an online service provider, we are not responsible for the conduct of our users, we want Facebook to be a safe place on the internet. Therefore, in using Facebook, you may not:

- Violate any local, state, national or international law or post any Content that would encourage or provide instructions for a criminal offense.
- Impersonate any person or entity or otherwise misrepresent yourself, your age or your affiliation with any person or entity.
- Use Facebook to send or make available any unsolicited or unauthorized advertising, solicitations, promotional materials, “junk mail,” “spam,” “chain letters,” “pyramid schemes,” or any other form of solicitation.
- Post or share any personally identifiable or private information of any third party.
- Solicit passwords or personal information from anyone, including those under 18.
- Use information or content you obtained on the Facebook website or service in any manner not authorized by the Facebook Code of Conduct or Terms of Use.
- Post any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
- Register for more than one account or use or attempt to use another’s account, service or system without authorization or create a false identity on the Service or the Site.
- Engage in any predatory or stalking conduct.

Source: www.facebook.com

2.5 SECOND LIFE



What is Second Life

Second Life (commonly known as *SL*) and its sister site *Teen Second Life* are Internet-based virtual reality environment that was launched in 2003 and developed by Linden Research, Inc

Second Life is exclusively for users aged over 18, while *Teen Second Life* is restricted to users aged between 13 and 18. A free downloadable programme called the Second Life Viewer enables its users, who are known as residents to interact with each other through motional avatars, providing an advanced social network service combined with general aspects of a metaverse (virtual universe). Residents can explore, meet other residents, socialise, participate in individual and group activities, and create and trade virtual items and services with one another.

Second Life's world (called "the grid") is divided into 256 x 256m areas of land, called Regions or Sims (short for "Simulators"). Each Region is simulated by a single server, and is given a unique name and content rating (either PG or Mature). The most basic mode of transport is by foot - walking, running, or jumping - but avatars may also fly unaided, ride in vehicles, and teleport (abbreviated to "TP") directly between locations. Land in Second Life is treated as a valuable and scarce commodity; residents can buy, sell, and rent land areas from each other. Mainstream media has focused on a small number of avatars who make large sums of money by doing so.

Built into the client is a simple primitive-based 3D modeling tool that allows any Resident to build simple virtual objects, and a scripting language called LSL ("Linden Scripting Language") which can be used to add autonomous behaviour to these objects. Other content, such as more complex 3D objects (called "sculpties"), textures for clothing or other objects, and animations and gestures, must be created using external software such as Blender, Poser, or Adobe Photoshop. The Second Life Terms of Service ensure that users retain copyright to any content they create, and the server and client provide simple Digital rights management functions. Content may be given away, or sold.

Second Life uses an internal currency called the "Linden Dollar" (L\$). L\$ are usually obtained via purchase for real money from other users; Linden Lab and others offers a brokerage service for these transactions. Users may also offer items or services to other users in exchange for L\$; services include "camping", working in stores, business management, entertainment (which prominently includes adult entertainment), custom content creation, and other personal services. Virtual goods include buildings, vehicles, devices of all kinds, animations, clothing, skin, hair, jewelry, flora and fauna, and works of art. Second Life's own subscription fees, which are based on the amount of virtual land a user owns, are charged in US\$; the exchange of L\$ for US\$ thus enables users who contribute content widely valued by other Residents to avoid paying US\$ from their own pocket to retain that content in the world. This is the most popular usage for the exchange of L\$ for US\$; in spite of attracting large volumes of press coverage, only a very small percentage of Residents derive a net income from the economy. The currency has become the subject of concern in economic circles in regard to possible taxation.

Safety Issues

There have been some cases in which users in Second Life were found to have been creating or exchanging child pornography, which has led it to be a common target for media outlets. This includes both real-life photographs and virtual recreations of pornographic scenes involving children, which are illegal in many countries.

Linden Lab has taken action by disallowing sexual ageplay (activities) between avatars, amongst other rule changes to police the issue. Banning the content directly is not possible, as such content can be created by having a child avatar run a sexual animation intended for adults; neither the avatar nor the animation is illegal (or against TOS) on its own, and their combination does not represent a separate asset.

The ban on sexual ageplay has caused difficulty due to the full customizability of Second Life avatars; there is no prescribed way to set or determine the age of an avatar, and it is easy to create an avatar which has the height and stature of an adult but appears child-like with regard to body development (or vice versa), and a person's belief regarding the age their avatar appears to be may not match the belief of other people.

A difficulty has arisen with the possibility of underage users accessing adult material on Second Life. Although the Terms of Service state that a user must be over 18 to register a *Second Life* (as opposed to *Teen Second Life*) account, there is no legal guarantee provided that all users of the world are over 18. An age-verification system was added enabling residents to further limit access to mature content. Virtual landowners may flag their parcels as "adults only" and block those that have not completed this process. Participation in this program is currently voluntary, though there is no assurance that this feature will always be so., and the program has raised further doubts concerning the need to disclose personal information to verify age and the actual effectiveness of such age verification. Finally, limiting access to a parcel only prevents the avatar entering the parcel; its content can still be viewed from outside by moving the camera.

A further concern is that, although the age verification process is voluntary, an account that has *not* been age verified can be instantly locked out of the world if another user files a report to Linden Lab that the owner of the account is underage. The user is then required to complete age verification or remain suspended from Second Life, losing all money and content they had in the world. Since the user cannot log in to Second Life, doing so requires them to contact Linden Lab by fax or postal mail or contacting the Support Portal at Secondlife.com.

Teen Second Life has developed the following Online Safety Tips for Teens and Information for Parents.

[Online Safety Tips for Teens](#)

Stay Anonymous

Don't ever tell anyone online your real full name, your parents' names, your home address, your school name or location, your phone/mobile numbers, social security & credit card numbers, and anything that shows what you look like such as a photo, video or webcam link. If someone asks you for this info don't give it to them and report the incident at *Help > Report Abuse*.

Keep your Password to Yourself

Friends don't ask friends to share passwords. If you give your password to someone they will have access to all of your account information and your inventory items. Not to mention, you'll be held responsible for anything they do while using your account. Linden Lab employees will never ask you for your password.

Don't Respond to Nasty Comments or Actions

If a mean or inappropriate comment or action is directed at you the best thing to do is ignore it and report it at *Help > Report Abuse*. You can use the Mute button on a Resident's profile window to ignore their chat. You can also Ban them from visiting land that you purchased.

Trust your Instincts

If someone makes you feel uncomfortable or threatened, use the Mute button on their profile window and report them at *Help > Report Abuse*. If you ever get really scared you should log off immediately. Don't worry about seeming rude. If someone is making you feel uncomfortable they're the ones being rude. Remember, in Second Life the exit is only a click away.

Keep your Parents in the Loop about your Second Life

Tell your parents about your Second Life friends and your favorite things to do in-world. Show them around every now and then. Don't be afraid to ask for their help when you need it.

Beware of Online Advice Givers

The best place to seek advice for really serious issues like depression, health problems, or trouble at home or at school is a trusted adult offline. Beware of anyone online who claims to be a counselor or therapist wanting to help you with these types of issues. They may not really have your best interests in mind.

If it Sounds too Good to be True it Probably is

Don't believe anyone in Teen Second Life who tells you they are a famous celebrity. You may really want it to be true, but it's best to be skeptical of these claims, especially if they ask for your password or for personal information. The same goes for anyone who tells you they are a modeling agent, music agent, or movie agent in real life.

Never Meet Offline

Teen Second Life friendships should stay in-game. Never meet any of your Teen Second Life friends' offline unless you are attending an official Linden Lab gathering with your parents.

If you have any further questions, you can contact us through the Second Life Support Panel at <http://secondlife.com/support/>

Information for Parents

How can My Teen get Help in Teen Second Life?

Linden Lab staff can be spotted in-world with the last name Linden and the title Liaison. Liaisons are always reachable via our in-world Instant Messaging feature.

How can I Share My Teen's Second Life Experience?

We encourage you to become involved in your teen's Second Life experience. Ask them to show you around the world and to keep you informed about their in-world social and creative activities. Because only authorized adults are allowed in Teen Second Life, we do ask that you not actively operate your teen's avatar yourself. However, if you enjoy your experience with your teen you are welcome to visit **Second Life's** separate world for adults where you can have an avatar and account of your own.

Is Teen Second Life Safe for My Teen?

Linden Lab is committed to providing a safe online environment for its teen residents. Teen Second Life will always be staffed with Liaison coverage during open hours. You can help your teen stay safe by teaching them never to reveal any personally identifying real life information while they are online. Read Linden Lab's **Online Safety Tips** for more suggestions about how to communicate safely online.

The Teen Second Life Community Standards apply to all teen community areas of Second Life, the Teen Second Life Forums, and the Teen Second Life Website. You should also take a look at the Terms of Service for more information about other actions that could result in account suspension or banning.

Are My Child's Personal Details Safe with Linden Lab?

At Linden Lab, we value your support and are committed to protecting your teen's privacy. We take precautions to make this site and the Teen Second Life virtual world safe environments for users. To learn more, please check our **Privacy Policy**.

Why Do You Ask for My E-Mail Address?

We ask for your e-mail address so that we can send password reminders, and account information as needed. If it is necessary to issue your teen an official Account Strike Notification, you will also receive it via email. We also offer you the ability to request up-to-date **Account Activity** summary information. In the future, Linden Lab will offer an opt-in newsletter to Teen Second Life Residents and their parents.

Does It Cost Anything to Play Teen Second Life?

A single Basic account is completely FREE, and includes access to events, shopping, building, scripting - everything you can do in Teen Second Life. The free Basic account is good for a lifetime of play. Start your teen with a **free account** today!

Why Can't my Teen be on the Second Life® World for Adults?

The Second Life world for adults is an exciting and attractive place, and some teens may be tempted to try to access it. However, the adult Second Life world is just that: adult. It is not intended for minors, and some of the content is geared toward mature users over 18 years of age. Linden Lab is committed to providing a secure environment for teen residents in Teen Second Life; to that end, violators of the adults-only policy of Second Life may face suspension and permanent ban from Second Life.

What if My Teen Wants to Acquire Land?

A Premium Teen Second Life account, starting at \$9.95 a month, allows your teen to acquire land on which they can build, display, entertain and live. Visit Virtual Land to learn more about purchasing land in Teen Second Life. The Land Use Fee is a monthly charge for the peak amount of Second Life land held during the previous 30 days in excess of the 512 square meter allowance granted with a Premium Account. The fee is tiered, and discounted as you acquire more land. When purchasing new land, you will be alerted if the new acquisition moves you into a higher tier requiring a greater monthly land use fee.

How Can I Get Further Information About Linden Lab's Second Life?

If you have any further questions about your teen's Second Life account, you can contact us through the Second Life Support Panel at <http://secondlife.com/support/>

Sources: www.secondlife.com and www.teen.secondlife.com

2.6 OTHER SITES



Friendster (www.friendster.com), Friendster is one of the biggest online social network with more than 90 million members worldwide. It focuses on helping people stay in touch with friends and discover new people and things that are important to them. Friendster prides itself in delivering an easy-to-use, friendly and interactive environment where users can easily connect with anyone around the world via www.friendster.com and m.friendster.com from any Internet-ready mobile device



MyYearbook (www.myearbook.com) is similar to other social networking sites and has become one of the top ranked destination sites for teenagers ages 12 to 17. The site was inspired by the typical yearbooks sold in high schools in America, but was intended to not only keep records of students but also allow them to keep in contact with one another. The site has added a number of features that are commonly found on other social networking sites but use different names.



Nimble (www.nimble.ie) is an Irish social networking site which is becoming increasingly popular. It is a social media network where members can stay in touch with their friends, share photos, view videos, play games, meet new people and just hang out.



Twitter (www.twitter.com) **Twitter** is a free social networking and micro-blogging service that allows its users to send and read other users' updates (otherwise known as *tweets*), which are text-based posts of up to 140 characters in length. Updates are displayed on the user's profile page and delivered to other users who have signed up to receive them. Twitter has become very popular with celebrities thus giving it a lot of media publicity in recent times. Senders can restrict delivery of their messages and updates to those in their circle of friends. Users can receive updates via the Twitter website, SMS, RSS, or email, or through a range of its applications such as TwitterMobile, Tweetie, Twinkle, TwitterFox, Twitterrific, Feedalizr, and also Facebook.



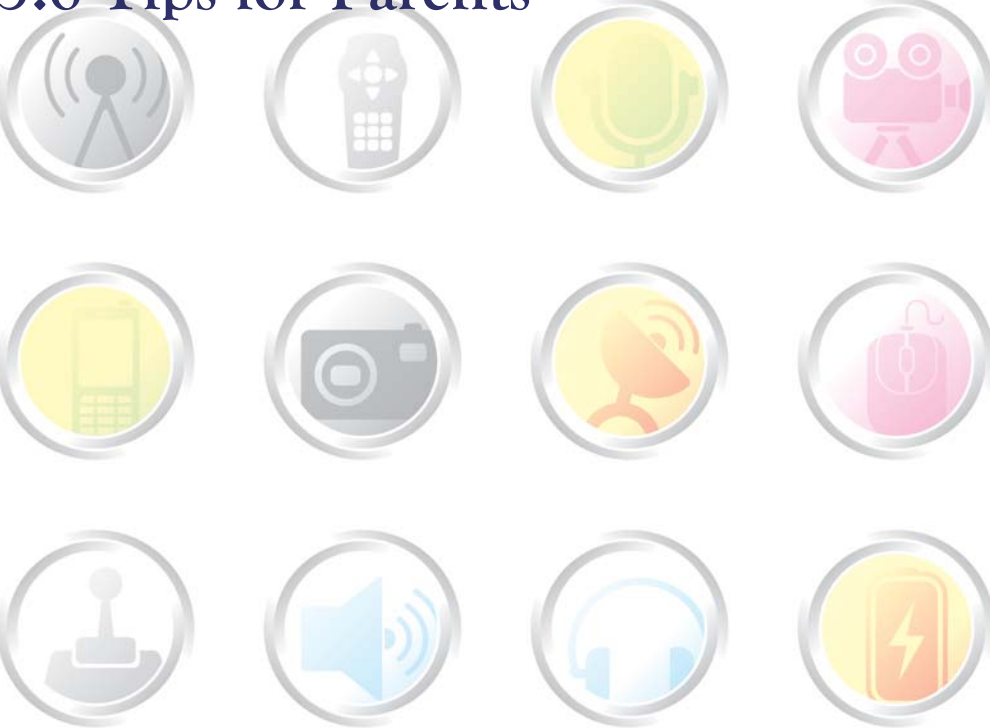
Xanga (www.xanga.com) began as a site for sharing book and music reviews. It now has an estimated 40 million users worldwide with a large focus on blogs. All Xanga members receive a "Xanga Site", a web site made up of a weblog, a photoblog, a videoblog, an audioblog, a "Pulse" (mini-blog), and a social networking profile. Members also have the option of joining or making blogrings (groups).

All of these well known social networking sites and others usually have good safety sections and complaint reporting mechanisms within their sites, which are worthwhile checking out if the young people you work with are using them



SECTION THREE: Cyberbullying

- 3.1 What is Cyberbullying?
- 3.2 What Makes Cyberbullying Different
- 3.3 Responding To Risk
- 3.4 Cyberbullying Safety Tips
- 3.5 Tips for Young People
- 3.6 Tips for Parents



3.1: WHAT IS CYBERBULLYING?

Cyberbullying is the use of electronic and digital means, particularly mobile phones, personal computers, email and Internet use to deliberately harass, ridicule or hurt another. It can be an extension of face-to-face bullying with Information Communication Technology (ICT) used to deliberately hurt someone else.

Cyberbullying is a method of bullying rather than a new type of bullying, after all abusive phone calls have long been used to intimidate and harass. However, the increasing use of mobile phones and the Internet by young people and adults alike provides the bully with another route to hurt a person.

Cyberbullying includes the following:

- Sending nasty, mean or threatening messages, emails, photos or film.
- Silent phone calls.
- Putting up nasty posts or pictures on a bulletin board, website or chat room.
- Saying hurtful things in a chat room.
- Pretending to be someone else in a chat room or message board or text message and say horrible things.
- Accessing someone's accounts to scare them or make trouble for them.
- Prolonged campaigns of harassment can occur, aimed at both students and staff, there are examples of school staff being ridiculed and abused online by pupils.

Bullying behaviour, by its very nature, undermines and dilutes the quality of education and imposes psychological damage. As such, it is an issue which must be positively and firmly addressed through a range of school-based measures and strategies through which all members of the school community are enabled to act effectively in dealing with this behaviour. Like all bullying, cyberbullying should be taken seriously.

Most youth organisations will already have Anti-Bullying policies, Behaviour Policies and their Acceptable Use Policies. Creating a positive and supportive ethos is perhaps the best preventative measure that can be taken against bullying in whatever form it takes. Encouraging friendships and developing the social skills of young people so that they can build self esteem and learn how to cope when a friendship falls apart and how to resolve conflicts in appropriate ways are life skills that youth organisations are very skilled in delivering to young people they work with.

3.2 WHAT MAKES CYBERBULLYING DIFFERENT?

Cyberbullying differs in a number of ways from other kinds of bullying – the invasion of one’s home and private space, the speed and scale of its impact, the possibility of it resurfacing in the future. However, it does produce evidence in a way that other forms of bullying do not.

- Communication between young people is often hidden from adults. This is exaggerated online where they are increasingly communicating in ways that are unknown to adults and free from their supervision.
- When they are online young people can hide behind the anonymity that the Internet can provide.
- The big difference between writing nasty messages to an individual and posting it on the Internet is the messages can be seen by a very wide audience almost instantly.
- Young people posting messages on the Internet do not feel as responsible for own their online actions as they do in ‘real life’ as they do not fear being punished for their actions.
- This type of behaviour is often outside of the reach of the youth organisation as it often happens on laptops/pcs at or via mobile phones.
- Young people are often fearful of telling others about being bullied because they fear that the bullying may actually become worse if they tell.
- They are often also afraid to report incidents, as they fear that adults will take away their mobile phone, computer and/or Internet access.
- In most cases, cyberbullies know their targets, but their victims do not always know their cyberbullies.
- Communications technology has become omnipresent, it is everywhere. As a result, Cyberbullying can happen any time and any place and for many young people, there is no longer any safe place if they are being bullied.

3.3 RESPONDING TO RISK

As with most safety issues, raising awareness of the issues and educating people to minimize the risks are the keys to safety. The more you know as a youth worker, parent or teacher, the more you can support your young people. Get them to talk about what they use the technology for – whether it is a mobile phone, a PC or a video games console. Your young people will enjoy the fact that they can teach you something and it is an opportunity to share activities with them. Spend some time informing yourself of the issues, you are already on the right track reading this article.

Webwise have developed a website called www.watchyourspace.ie to enable young people to take control of their online lives and give them the advice and resources to deal with the fallout from misuse of mobile phones and social networking sites. **Watchyourspace** encourages the keeping of texts or chat comments to aid any investigation. It demonstrates how to access reporting routes to social networking sites and mobile phone companies and internet service providers, the Gardáí and the Hotline for the reporting of illegal use of ICTs. It also links to Childline online allow young people to make contact with a Childline counsellor if they would like to talk about a problem.

3.4 CYBERBULLYING SAFETY TIPS

Discover the Internet Together, Be the One to Introduce Your Young Person to the Internet.

For both parent and young person it is an advantage to discover the Internet together. Try to find web sites that are exciting and fun. Hopefully you will together achieve a positive and conscious attitude to Internet exploration, which again could make it easier to share both positive and negative experiences in the future.

Encourage Your Young Person to be Careful when Disclosing Personal Information

Being conscious of when and where it is all right to reveal personal information is vital. A simple rule could be that the young person should not give out name, phone number or picture without your approval. Never give out or share personal information numbers (PIN), etc.

Teach Your Young Person About Source Criticism on the Net

Most young people use the Internet to improve and develop knowledge in relation to schoolwork and personal interests. Net users should be aware that not all information found online is correct. Educate young people on how to verify information they find by comparing to alternative sources on the same topic.

Encourage Good Netiquette

Netiquette is the informal code of conduct for the Internet. As in everyday life, there are informal ethical rules for how to behave when relating to other people on the Internet. These include being polite, using correct language and not yell at (write in capital letters) or harass others. Also, young people as well as grown ups should not read other's e-mail or copy protected material.

Know Your Young Person's Net Use

To be able to guide your young person with regard to Internet use, it is important to understand how young people use the Internet and know what they like to do on-line. Let your young person show you which websites they like visiting and what they do there. Acquiring technical knowledge could also make it easier to make the right decisions regarding your young person's Internet use.

Remember that the Positive Aspects of the Internet Outweigh the Negatives

The Internet is an excellent educational and recreational resource for young people. Encourage your young person to be conscious and explore the Internet to its full potential.

3.5 TIPS FOR YOUNG PEOPLE

Do trust your instincts. If it doesn't look or "feel right", it probably isn't. If you find something online that you do not like or makes you feel uncomfortable, turn off the computer and tell an adult.

Do not keep this to yourself! You are NOT alone! Tell an adult you know and trust!

Do not delete messages from cyberbullies. You do not have to read it, but keep it, it is your evidence.

Don't send messages when you are angry. It is better to wait until you have had time to calm down and think. You will usually regret sending a "Flame" (angry) to someone else. Once you've sent a message, it can be very hard to undo the damage it may cause.

Don't open messages from people you don't know.

Don't reply to messages from Cyberbullies. Even though you may really want to, this is exactly what cyberbullies want. They want to know that they've got you worried and upset. They are trying to mess with your mind and control you, to put fear into you. Don't give them that pleasure.

3.6 TIPS FOR PARENTS

As with all other Internet safety issues one of the biggest positive impacts on young people's online behaviour will be caused by active engagement by parents in their online life. Remember the chances of a young person sharing their online experiences with you will be greatly reduced if they think that telling you about a problem will result in them being banned from using the Internet.

Build Up Your Knowledge

Get your children to talk about what technology they use and what they use it for – whether it is a mobile phone, a PC/laptop or gaming console. Hopefully, they will enjoy teaching you something and it is an opportunity to share activities with them.

Encourage Your Child to be Careful when Disclosing Personal Information.

This is obvious and applies to all areas of Internet use and is especially important when using social networking sites. A simple way to explain this to your child is that they should not supply any information, photos or images online that they would not be happy to give to a stranger they met on the street.

Encourage Respect for Others

As in everyday life, there are informal ethical rules for how to behave when relating to other people on the Internet. These include being polite, using correct language and not harassing others. Make your child aware that despite the perceptions to the contrary, online bullying is easier to detect and trace than offline bullying. Online bullying can have more severe consequences for the victim because it is so difficult to escape from. Also because of the code of practice adopted by Internet Service Providers and mobile phone operators, companies are obliged to involve the Gardaí when illegal activity is reported to them.

Know Your Child's Net Use

To be able to guide your child with regard to Internet use, it is important to understand how they use the Internet and know what they like to do online. Let your child show you which websites they like visiting and what they do there.

Online Shorthand

It is also useful to be aware of the shorthand abbreviated language that is often used in online talk to keep conversation and communications private between users. Some of the most commonly used are the following:

ASL – age, sex location

F2F – face to face

K4Y – kiss for you

LMIRL – let's meet in real life

OLL – online love

PAL – parents are watching

POS – parents over shoulder

WYCM – will you call me

BBB - bye bye baby

KFY – kiss for you

KPC – keeping parents clueless

LY4E – love you forever

PAL – parents are listening

PIR – parents in room or people in room

WTGP – want to go private



SECTION FOUR: Other Issues



Introduction
4.1 Instant Messaging

4.2 Using Mobile Devices

4.3 Online Gambling

4.4 Use of Credits Card Online



4.5 Gaming Issues



INTRODUCTION

There were a number of other areas of Internet/I.T usage, some related to the use of social networking sites and some not which were raised as a concern during the consultations with youth workers in developing these guidelines. Some of these while not specifically aligned to social networking were not covered in the original Safe Surfing guidelines. Therefore, it was deemed important to include them to make people aware of the safety/risk issues involved with the following: Instant Messaging; Using Mobile Devices; Online Gambling; Using Credit Cards Online and Online Gaming.

4.1 INSTANT MESSAGING

What is Instant Messaging?

Instant Messaging, or IM as it is often referred to consists of sending real time messages to another Internet user. Instant messaging can be compared to chatting to someone in your own private chat room, with only those people you choose to invite. Instant messaging is a bit more private than a typical chat room, and it is a much faster and simpler way to communicate than using email which makes it attractive to young people. It allows users to communicate in real time and respond quickly to questions or comments similar to texting on a mobile phone. Instant messaging also allows the user to save money as it is cheaper to communicate long distance in this way rather than by phone.

You can create a list to keep track of welcome guests and alert you when one of them sends you a message.

As with any online activity, caution should be exercised with messaging. It is not a good idea to add people to your list unless you know something about them. Children should be supervised carefully when instant messaging and should never add someone to their list or agree to be added to anyone else's list without approval from their parents. Predators have been known to use instant messaging as well as chat rooms to seek out victims, so while IM may seem safer, it is not without risks.

It is also possible to obtain viruses, worms, and Trojan horses through messaging, so care should be taken when accepting any files. Also, don't type anything that you wouldn't want shared with others, since IM's can be captured and the text can be saved. Even though messaging sessions seem private, they are really not any more secure than your average email. Instant messaging can be a lot of fun and it is a great way to communicate, but like anything else, it should be used with care

Using instant messaging (IM) to send and receive messages and/or files and images, is very similar to using e-mail or SMS messaging and some of the same safety rules apply. Your instant messaging program can be a direct link between you and spammers, scammers, identity thieves, online predators and cyberbullies. On this page you will find some basic tips on instant messaging safety:

Basic Safety Tips for Instant Messaging

- Choose a non identifiable, non gender specific screen name (and keep it clean!)
- IM screen names, like e-mail addresses, should be kept private. If you post your e-mail address on line, you are making yourself a target for unsolicited e-mail and if you post your IM screen name then you are making yourself a target for unsolicited IM messages, sometimes referred to as spim.

- IM usually allow you to control if people on your contact list can see if you're online. That means you can set your IM client so that when you log on, nobody can see you giving you time to check out which of your contacts are online and, if there are any "mysterious" contacts you don't recognise.
- Never give out any personal information whilst using IM. That means your real name, telephone or cell phone number[s], mailing address, passwords, banking details etc. Remember, with many IM clients, your screen name can be used to identify your e-mail address
- You should only communicate with contacts you recognise, if someone you do not know sends you a request to add them to your contacts, decline it and block them until you are sure you know who that person is.
- If you plan to ask someone if you can be added to their contact list, make sure they know you are going to do that by e-mailing them and/or asking them first.
- Never accept files or downloads from people you don't know or from people you do know, if you weren't expecting them. This includes URLs.
- Never arrange to meet someone offline that you only know through IM conversations.
- Make sure you know how to save copies of your IM conversations.
- Remember your Netiquette and be nice! Don't send mean IM messages or incite others to do so.
- When you are not available to receive messages, be careful how you display this information to other users. For example, you might not want everyone on your contact list to know that you're "Out to Lunch."

Using Shared computers

- If you use a shared or public computer (at home, work or school/college, for instance) do not use the automatic login that comes as standard with most instant message programmes. People who use that computer after you may be able to see and use your screen name to log on.
- If you use a computer at work, your company may have the right to view your conversations so don't use your work computer for private IM conversations.

These are not the only safety issues related to using Instant Messaging. In addition to privacy, it should also be noted that Instant Messages are transmitted as clear text, using insecure protocols and that these messages use nonstandard TCP ports, so will not necessarily be filtered by firewalls. Depending on your antivirus software, IM attachments may not be scanned for viruses.

It is important to remember that, in order for your Instant Messaging to be secure; your computer must also be secure. It is vital that you run up-to-date antivirus software and that you regularly apply security patches to your computer. You should also install either a software or hardware (or both) firewall to add extra protection for your computer.

4.2 USING MOBILE DEVICES

It is important to be aware and safe online at all times while you're using the Internet whether it be at school, work, home, or even on an Internet enabled mobile device such as a mobile phone, smart phone or a wireless personal digital assistant (PDA). Users with mobile devices such as mobile phones will have much of the same access and features available on a desktop or laptop computer. The same basic safety rules and tips apply when you access social networking sites and the Internet from mobile devices, but there are also extra precautions to be considered when using the Internet



Stop and Think Before Uploading Images.

Some mobile devices let you upload photos straight from the camera on your phone to the Internet. Although this may be a quick and easy way to share new photos, stop and think about what you are putting up before posting. Be sure that the photos uploaded are appropriate without sexually explicit or inappropriate material or showing identifying characteristics that would allow someone to find you in the real world or will portray you in a way that you will not be happy about. Be aware also that you could be putting up images of other individual without their permission which they may not be happy about.

Don't Save Login and Passwords on Mobile Devices.

Given their portability, mobile phones and devices can be easily lost or stolen. If your login and password are saved on your mobile device anyone who may have possession of that device can access your profiles, friends, photos, etc. If your device is lost or stolen, immediately change your passwords on any social networking sites and call your carrier to deactivate the device.

Be Aware of Your Environment.

No matter where you are accessing the Internet on your mobile device, look around to see who may be watching you or trying to see what you are doing. Put your mobile device away if someone you do not know is trying to see your profile or personal information without your consent.

4.3 ONLINE GAMBLING

Online Gambling

Ireland has a long established culture of gambling through the horse and greyhound racing industries, which for many is an integral part of Ireland as a sporting nation. However, online gambling is a relatively new form of gambling which has exploded in recent years and has become a multi billion euro industry. Online betting is rapidly taking over from betting shops as the primary method for people to have a bet and online poker and has become very popular with young men in particular.



Most people who play poker or other games or who like to gamble do not develop gambling problems. However, electronic/online gambling is now being considered the most addictive type of gambling. In fact, these games are so addictive they are often referred to as the '*crack cocaine*' of gambling.

The reasons for this are that they are played in isolation with complete privacy, can be played very quickly, and there is no time limit for most online forms of gambling. There is also the added danger of playing with what can appear to be an unlimited amount of 'virtual' money via a credit card.

While a majority of young people will not have problems when they gamble, more young people are developing problems with gambling. A range of international studies have shown that somewhere between four and eight percent of young people who gamble develop a gambling problem with an additional 15% being at risk for developing a gambling problem. Within the broader debate on safe social networking and the use of the Internet online gambling is an emerging issue that has been specifically identified by youth workers as an area of concern.

The consequences of problem and addictive gambling include more than the debts incurred or what a young person will do in order to service these debts. Depression, social withdrawal, and school dropout are just a few of the recognised consequences of a gambling problem.



Legal Position

In America the law prohibits the use of credit cards for online gambling sites, thus establishing more of a barrier for young people. However, this does not exist in Ireland and the existing legislation is extremely outdated with the Gaming and Lotteries Act of 1956 (amended in 1979) still the primary piece of state legislation in operation.

New legislation on gambling is due to be looked at by Government both to deal with the existing outdated legislation and to deal to the possibility of large casinos coming to Ireland (although many small casinos are already in operation which are not properly licensed or legislated for).

Responding

In terms of what a worker or parent can do, the principles are similar to those previously outlined on the use of credit cards.

If as an adult you have given access to or supplied details of a credit card to a young person it is important to ensure that this trust has not been abused and that it has been used only for the purpose for which the card or the card's details were made available. Regular checks on the credit card balance which can be done very quickly through online banking are the easiest way of monitoring this.

In the case of a young person with their own credit card and of legal age to gamble then personal responsibility the principles of good money management can be stressed.

It is important that young people are aware of the potential dangers of online gambling and how quickly debt can be built up. Running gambling education and awareness programmes/sessions can be very effective in the same way as drug/alcohol/sex education programmes are used.

4.4 USING CREDIT CARDS ONLINE



Setting yourself up on a social networking site or availing of particular services on these sites can in some cases necessitate the use of a credit card. In the case of someone under 18 years of age this will normally require gaining access to and/or permission to use an adult's credit card. It is important therefore to be aware that subsequent to this the young person may have all the details required to use the credit card online.

Online shopping and online gambling (see below) have undergone similar increases in their popularity in recent years to that of social networking sites. The danger of dealing in what appears to be 'virtual' money is all too real and significant expense and debt can be incurred in very short periods of time.

If as an adult you have given access to or supplied details of a credit card to a young person it is important to ensure that this trust has not been abused.

Regular checks on the credit card balance which can be done very quickly through online banking are the easiest way of monitoring this.

In the case of a young person with their own credit card personal responsibility is obviously paramount but it is important that they are aware of the potential dangers of using credit cards online.

4.5 ONLINE GAMING ISSUES

What Is Online Gaming?

An online game is a digital game that uses a live network connection in order to be played, which usually means the internet. So, this includes games played on the Internet, from simple games (e.g. puzzles or word games) to Massively Multiplayer online role playing games (MMORPGs), but also those played online through consoles, across mobile phones or via peer-to-peer networks. The online element of gaming is still relatively new, however, its popularity is increasing with Internet access and readily available broadband technology and it is predicted to expand dramatically in the next few years.



A relatively new but growing phenomenon amongst children and young people, online games present new and different kinds of opportunities and potential risks to games played offline. Many of these are similar to the benefits and risks of internet use generally, as online gaming merges issues of content, contact and conduct online. With its changing nature and the possibility for user generated content, it is equally difficult to regulate.

Online gaming is usually done through a games console, a portable gaming device or a Personal Computer. PCs and the current generation of games consoles (including portable consoles with wireless connectivity) allow players to create an account and connect their console to the internet. Players either buy games from high street or online retailers, or download games digitally online. Games can then be played online with other players who have the same set up

Massively Multiplayer Online Roleplaying Games (MMORGs)

MMORGs are one type of online game, usually played via a PC but some can also be played via games consoles. Typically, these games present three-dimensional virtual worlds in which thousands of gamers assume the roles of fictional characters ('avatars'). They tend to provide a more open-ended approach to gaming, and are notable for their social nature and community aspects that surround game play. They differ from other online games in the large number of concurrent players participating in a single game and the persistent and immersive nature of the games (i.e. play continues whether a particular gamer is participating or not). A recent survey suggested that 25% of players of massively multiplayer online role-playing games are under the age of 18, most players play with somebody they know in real life, and that on average players spend 22 hours a week in the environment.

What are the Benefits?

There are numerous benefits to being able to play video games online. They enable children to play with friends, family, or people they meet online, whether other players are just down the street, or on the other side of the world. Often, they can communicate in real time, either through instant messaging or via "chat" functions, using a microphone and headphones. They provide a social tool which offers another opportunity to meet new people and interact anonymously and openly, which can help with identity exploration in adolescents.

There is also excitement about the learning potential of these games and the experiences of running 'guilds' or 'clans' (teams of characters within a game) as potentially reflecting managerial & social skills required in the real world. Online gaming is an important part of the lives of many children and young people with specific accessibility needs as they offer a platform where players enter into the arena on a level playing field. For example, children with disabilities who might otherwise need supervision from a carer in many other real world activities.

What are the Risks?

The risks involved in online gaming generally reflect the risks of going on the Internet more generally. As such, much of the attraction and benefits of online gaming, such as playing somebody you don't know, can be the very things that can create the potential risks. They include issues of – content; contact; conduct; and excessive use.

Content: Not only 'static' content which the commercial developer created, which can be reliably rated, but also potentially inappropriate material that is user generated – therefore less controllable and which can evolve, making games ratings not wholly effective. In addition, users will be increasingly able to use games devices to share and create content, some of which could be age inappropriate or offensive.

Contact: Giving away personal details, for example, through instant messaging & chat functions when playing games with players that you meet online and don't know in the real world. This has the potential to lead to incidents such as grooming and cyberbullying. Also, links to other sites & adverts that may not be appropriate.

Conduct: Of children themselves and of other, often unknown/anonymous players (e.g. racist; sexist or other abusive or threatening comments, or bad language) that may be inappropriate for younger players.

Excessive use: In a recent study which looked at the kinds of problems young people encounter through too much playing of computer games, in particular a popular MMORPG, young people reported a number of impacts from excessive gaming. These included their eating habits being disturbed, staying up late at night due to the global nature of the game that cut across time barriers, encountering problems at school, and sometimes not having time for such everyday tasks as personal hygiene. The young people interviewed said this led to rows with their parents and their friendships and relationships also suffered. Players in the same study talked about what drives them to play for so long. These include different social pressures, such as feeling left out when playing is linked to friends and classmates outside the game, or feeling obliged to adapt to the playing habits of others to keep up. The game design and mechanisms which call for playing with other users, playing for long periods of time, and not being able to pause a game without disrupting game play were also seen as contributing to longer play.

Managing the Risks of Online Gaming

A number of different approaches are currently being taken to help manage the risks of online gaming. These include:

1. Labelling and age-rating of online games;
2. Restricting access: through parental controls on consoles and PCs, and age verification systems;
3. Moderation, including incentivising good behaviour and enabling reports of abuse.

1. Labelling and Age Rating Online Games

The current age ratings and accompanying information descriptors are also used for games that can be played online. One difference is that games provided purely online (e.g. where there is no physical disc) do not fall within the statutory classification, so games with extreme content rely on being voluntarily rated. However, at present, these games are generally not produced for adult audiences, and where they are, they are voluntarily classified.

The Pan-European Game Information (PEGI) age rating system was established to help European parents make informed decisions on buying computer games. It was launched in spring 2003 and replaced some national age rating systems with a single system now used throughout most of Europe. For online game play service

providers to obtain PEGI-online licences, they must sign up to the PEGI Online Safety Code, of which the main provisions are:



Age ratings – Only games with recognised age ratings will be included on a site

Reporting – Appropriate mechanisms are in place for players to report undesirable content, including on any related websites

Content removal – Licence holders will use their best endeavours to ensure online services under their control are kept free of content which is illegal, offensive, racist, degrading, Corrupting, threatening, obscene or which might permanently impair the development of young people

Privacy – Licence holders collecting personal information will maintain effective and coherent privacy policies in accordance with European Union and national Data Protection laws

Community standards – Licence holders will prohibit user generated content or conduct which is illegal, offensive, racist, degrading, corrupting, threatening, obscene or which might permanently impair the development of young people

Advertising – A responsible advertisement policy must be in place

2. Restricting Access

There are a number of mechanisms that can be used to manage children and young people's access to game playing online:

Parental Controls: As described above parental controls on PCs and the latest generation of games consoles can give parents the tools to manage the level of children's access to online gaming – for example, by not allowing it at all, or controlling who they can play with; or deciding whether chat functions are allowed etc.

Age verification: In addition, where content is provided that may not be suitable for some children and young people, games websites often put systems in place for users to register their age. This is often by asking the player to key in their date of birth. Some sites try to incentivise children to tell the truth about their age by putting *upper* age limits on accessing certain material or linking access by under-18s to real world networks such as schools. Others require the user to register using a credit card.

Community approaches to managing risks: Typically, most online gaming hosts require that players sign up to user 'codes of conduct' governing basic interaction in games and on forums. Whilst they differ from game to game, there are some fairly standard elements, and usually include agreement for players not to:

1. Threaten other players;
2. Communicate players' real world information;
3. Use or post links to sexually explicit, abusive, obscene, hateful or offensive imagery, language or other content;
4. Violate any laws;
5. Modify official sites.

In addition, players often set their own codes of conduct that are relevant in their own gaming environments. To a large extent this kind of community moderation and management approach is similar to that used on social networking and other user generated content site discussed in the previous chapters.

3. Moderation and Reporting

In order to address non-compliance with player codes when it occurs and to minimise some of the potential risks involved in online gaming, most game website hosts offer some level of moderation. This can be in the form of in-game moderation (e.g. when a moderator appears as a character in a game, or when tools are used to detect inappropriate material), out of game moderation (e.g. responding to reports from users), as well as moderation of associated forums.

Online game hosts employ different techniques in order to identify content which may be inappropriate. These include using automated filters that recognise key words and phrases and blocking of inappropriate content such as email addresses, passwords and offensive language. Some also include mechanisms such as pop ups that remind users not to reveal personal information while they type. This content is then flagged for the attention of the sites moderators.

Source: Safer Children in a Digital World: The Report of the Byron Review. You can download this publication or order copies online at: www.dcsf.gov.uk/byronreview

© Crown copyright 2008

Xbox and PS2

When gaming is mentioned most people with even a basic knowledge would automatically think of either Playstations or Xbox and both

Playstation Safety



The principle of safe practices when using Playstation, particularly online, are very similar to general online safety. The following tips are recommended by Electronic Arts. Electronic Arts is one of the world's leading independent developer and publisher of interactive entertainment and games software for console systems.

Being online can be fun, sociable and inspiring. At EA we want you to enjoy the time you spend online at our sites and using our services. For that reason, we've prepared a few tips to help you stay safe when online. It is important that when you chat, use instant messenger (IM), or participate in other forums, you keep the following things in mind:

- 1. Be Discreet.** The information you provide is often public, for all to see. Do not share information or images that you do not want the world to know about or see. Think – your information could be passed on.
- 2. Be Anonymous.** Do not share private or very personal information. Never post or send anything that can be used to locate you or another person offline, such as a full name, email or home address or phone number.
- 3. Be Distant.** Do not arrange to meet in person anyone you've met online. If you must, only meet somewhere that is safe and public, tell someone your plans and then bring a friend along. If you aren't an adult, get your parent or guardian's permission first and take them with you.
- 4. Be Honest.** You may be tempted to pretend to be someone you are not. The other person may also do the same thing. They may not be who they say they are.

5. **Be Nice.** Don't take on bullies or cyber-bully anyone else. If someone taunts you, walk away from the computer. Report the person or behaviour to an adult or administrator. It's supposed to be fun, right?

6. **Be Clean.** Do not open, respond to or forward an email or IM unless you know the person who sent it to you and you've checked it for viruses. The content could contain damaging software (such as spyware or viruses) or it might be offensive.

7. **Be Secure.** Use security software (such as virus scanners). Ensure your system is up-to-date and protected in case an email from someone unintentionally infects your computer.

8. **Be Private.** Never share your password or password hints with anyone.

9. **Be Inventive.** Ensure the online IDs you create do not reveal your personal information. Be creative and unique!

10. **Beware.** If something sounds too good to be true, it probably is! Check the facts if you aren't sure about something. And remember – you're in control. You decide which activities to participate in and what information you provide.

Source: www.electronicarts.ie/pages/6469/

If when using Playstation you find someone is spoiling it for you, by cheating, harrassing or hassling you, intimidating you or threatening you in one of our games with malicious or offensive behaviour, there is a reporting site available at: <http://ie.playstation.com/help-support/grief-reporting/>

Xbox Safety



There is a facility in Xbox called **Family Settings** which perform two functions on the Xbox 360 console for playing offline and online. When playing offline, they can be set to grant or restrict access to games based on the ESRB (Entertainment Software Rating Board) rating. When playing online, they can be used to restrict access to content and contacts based on the parent's choice. Xbox LIVE Family Settings set different levels of protection for online gameplay, online communications, and downloading member content or items from Xbox LIVE Marketplace. Xbox LIVE Family Settings let you:

- Control access to all the features of Xbox LIVE.
- Set a pass code to protect your Family Settings.
- Decide what your kids will play, both online and off.
- Decide who your child can communicate with online.
- Control who can see your child's profile or friends list.
- Managing Xbox Live Activity

To access this from the System area of the Xbox Dashboard, select Family Settings, Xbox Live Controls. Xbox LIVE Controls come into play only when you take Xbox 360 online, and they are linked to a child's gamer profile and gamertag. When an Xbox LIVE account is created, the service asks for the member's age to determine whether to apply Family Settings to that account.

Parents are also required to create or use an existing Windows Live ID. The Windows Live ID is associated with the child's Xbox LIVE account and protects the settings from being changed later by the child. To change a child's settings, first select the child's account name and connect to Xbox LIVE. Once signed in, enter your Windows Live ID password to unlock the settings. Xbox LIVE Controls settings include:

Online Gameplay: Before you can play multiplayer games online, you need an Xbox LIVE Gold Membership. Once that's in place, this option allows you to decide if your child can play Xbox 360 games online as well as original Xbox LIVE-enabled games that are Xbox 360 compatible.

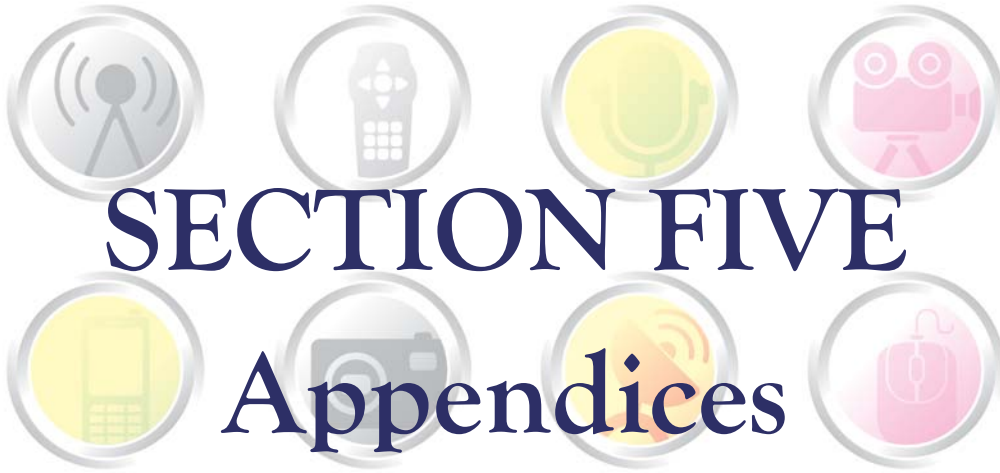
Privacy and Friends: You have the power to approve your child's online friends. Let your child communicate with anybody, or only with their friends; decide who can see your child's personalized gamer profile; decide whose gamer profiles your child can see; control who sees your child's online or offline status; and decide whether other people can see your child's friends. *Note - Your child's name, location, and bio are visible to anyone you allow to view your child's gamer profile.*

Voice and Text: Select "Everyone" to allow your child to communicate using voice and text with anyone on Xbox LIVE. Select "Friends Only" to allow your child to communicate only with people on their friends list. Select "Blocked" to prevent everyone from communicating with your child. No matter what the setting, your child will still be able to receive new friend requests for you to approve or block.

Video: Select "Everyone" to allow your child to communicate using video chat with anyone on Xbox LIVE. Select "Friends Only" to allow your child to communicate only with people on their friends list. Select "Blocked" to prevent everyone from communicating with your child.

Content: Content controls help you set limits on the kind of downloadable goodies your kids can access. You can choose to allow your child to peruse Xbox LIVE for downloadable game updates, demos, and other content, as well as whether your child can download member-created content from other Xbox LIVE members.

Source:<http://www.xbox.com/en-S/support/familysettings/live/xbox360/preNXE/xboxlivecontrols.htm>



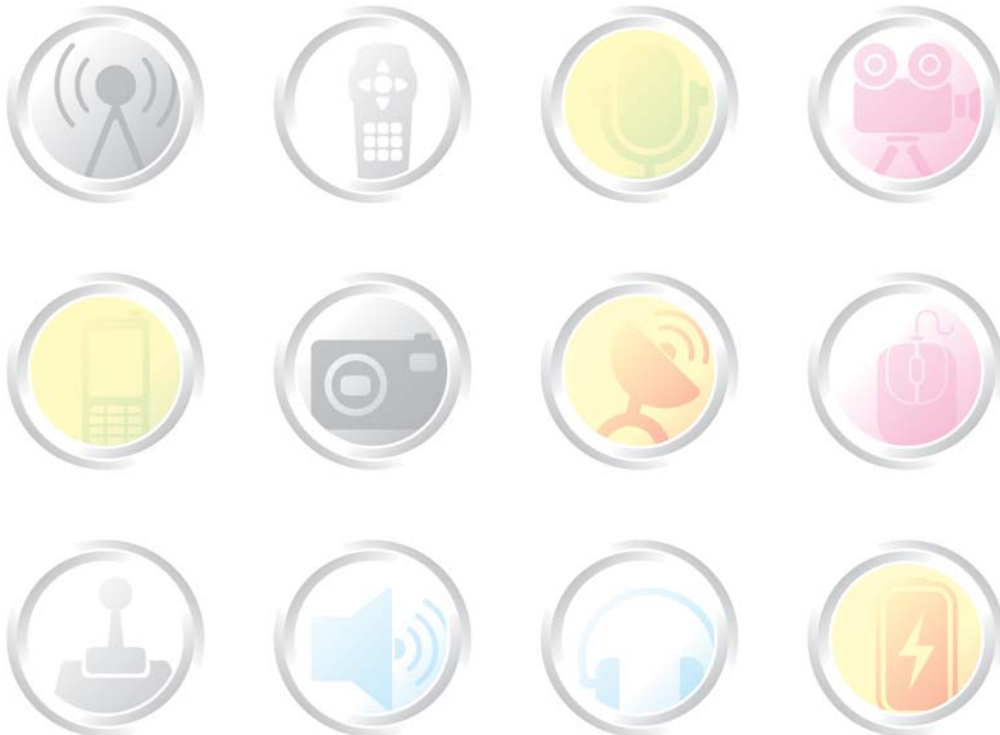
SECTION FIVE

Appendices

5.1 Acceptable Use Codes & Policies

5.2 Resources

5.3 Relevant Legislation



5: 1 ACCEPTABLE USE CODES & POLICIES

Many organisations schools, colleges, youth work settings etc. operate AUPs - Acceptable Use Policies - as a mechanism for ensuring the safe use of the Internet and IT equipment. A number of these are included in the Safe Surfing guidelines (*add link*) and a sample one is also included in this section.

The Acceptable Use Code below by BECTA (British Educational Communications and Technology Agency) is slightly different to many AUPs in that it focuses on responding to an incident when it occurs. This is an identified area of concern for youth workers as dealing with an inappropriate incident when it occurs is usually the time when youth workers are most likely to be faced . BECTA is the government agency in Britain leading the national drive to ensure the effective and innovative use of technology throughout learning.

Although it is school focused and based on the British formal education structure and legislation it provides a very comprehensive approach to dealing with an incident when it occurs and would certainly be adaptable to a youth work setting.

5.1.1. BECTA - RESPONDING TO INCIDENTS

Responding to Incidents

Even when schools have all the necessary policies and technological solutions in place, there may still be occasions when misuse of the internet and related technologies occur. Schools must ensure that they have appropriate strategies for responding to such instances.

Dealing with Incidents

Senior managers in schools are required to respond to a wide variety of incidents on a daily basis. Most of these incidents are minor, but some are more serious. The majority involve students, but on occasion it may be a teaching or non-teaching member of staff whose conduct is in question. Schools generally work from procedures which are based on school policy and established practice to deal with such incidents. However, responding appropriately to a breach of e-safety can cause some uncertainty, sometimes over what the nature of the offence may be, or even because of a lack of understanding of the potential seriousness of incidents involving technology.

The following section provides some examples of ICT-related incidents which schools might encounter, and suggests some strategies for dealing with them:

- Minor incidents
- Minor incidents of misuse by pupils might include:
 - Copying information into assignments and failing to acknowledge the source (plagiarism and copy right infringement)
 - Downloading materials or images not relevant to their studies, in direct breach of the school's acceptable use policy
 - Misconduct associated with student logins, such as using someone else's password
 - Incidents involving pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or moving.

Schools will have their own rules about particular technologies, and, in theory, many of these issues should have been covered within the school's acceptable use policy. In all but the most minor of cases it would be wise for the pupil to be issued with a warning, and the incident documented. If the behaviour is repeated, or the misconduct escalates, it can then be responded to more seriously if the school has evidence of previous events. Any incident of racially motivated abuse via technology needs to be linked in with the monitoring of racial incidents in the school.

The e-safety co-ordinator should monitor minor incidents to identify trends in pupils' behaviour, and should react proactively to any emerging issues. This might include raising awareness on a particular e-safety topic at a school assembly or offering staff additional training. It is also wise to periodically review the school's e-safety policies, and, in particular, acceptable use policies, to see if they should be modified in any way.

Incidents Involving Inappropriate Materials or Activities

While not illegal, there will be some material that is just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people.

Examples might include soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes, cartoons, or material which is used in low-level harassment.

Specific breaches of policy and rules might include deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network. Even if such material was not deliberately accessed by the pupil, but not reported to a teacher, and was subsequently shown to other students, this should also merit a disciplinary response.

Other incidents of more serious misuse by pupils might include cheating in an examination or plagiarism in coursework, which, aside from infringing school assessment policies, may have legal implications (for example, they may breach copyright law). Hacking, virus attack, chronic truancy (as a result of obsessive or excessive use of the internet and related technologies) and online gambling are all serious concerns for schools, and require a disciplinary response.

Age-restricted material is potentially more serious. Publications are classified to provide information and protect people from viewing material that might be inappropriate or damaging to their moral and physical wellbeing. It is therefore illegal to show, give or sell restricted materials to a person under a certain age. Blatant, intentional exhibiting of age-restricted materials to pupils under the specified age is a serious breach of e-safety and should invoke a strong disciplinary response from the school.

Incidents that involve inappropriate but legal material should be dealt with by the school via the usual disciplinary system; unless a criminal offence has been committed, it is not normally necessary to involve the police.

Incidents Involving Others

Any incident involving a member of staff is a serious, and often complex, matter. There may be implications for the safety of pupils, fellow employees and the learning environment, and for the reputation of the school. Schools should, in the first instance, ensure that they have an acceptable use policy for staff and that policies and procedures are in place should incidents occur.

Harassment of another person using technology, or breaching their right to privacy, poses a serious threat to their physical and emotional safety, and again may have legal consequences.

Depending on the nature of the incident there may be breaches of other school policies, such as the anti-bullying policy, which may also warrant review. Disciplinary action may range from a warning to dismissal of a staff member or suspension of a pupil.

As in all disciplinary instances of this seriousness, a school must be careful to follow disciplinary protocols, ensuring that proper documentation and recording of information occurs, and that appropriate counselling and support are given, and ensuring that parents and carers of the pupil involved are kept fully informed of the matter.

Dealing with More Serious Incidents

More serious incidents relating to e-safety in schools should be reported to the e-safety co-ordinator immediately. The e-safety co-ordinator must document the incident and decide on an appropriate course of action, which may include involving the head teacher and external agencies. It may also be necessary to involve the Local Safeguarding Children Board (LSCB) or child protection staff to provide follow-up counselling and support to both the victims and perpetrators. The e-safety co-ordinator should review e-safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.

If police involvement is necessary, it is advisable for the head teacher to seek legal advice, via their local education authority, as soon as possible.

Any serious incidents could become the subject of media attention. Schools should ensure that they have an appropriate strategy in place for dealing with media requests, and ensure that ongoing investigations and the continuing safety of the school are not compromised by media coverage.

Incidents Involving Illegal Materials or Activities

In the school context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by staff and pupils alike.

Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.

The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar antisocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as 'alarm', 'distress' or 'torment' fit the term most accurately, and some adverse impact on the victim is required. To constitute a 'course of conduct', harassment must take place on a minimum of two occasions.

What to do in the Event of Discovery of Indecent Material

Discovery of indecent material within the school's network is a very serious situation, and must always be

reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off. It may be necessary to shut down the whole network, but do not do this unless instructed by the police. Ensure that everyone is kept away and that nothing is touched.

Under no circumstances should the e-safety co-ordinator, network manager or head teacher attempt to conduct an investigation of their own, or bring in an outside 'expert' to do so, as this may compromise the evidence if a legal case were to result. In some cases this may constitute a criminal offence in itself.

In cases of pupil or staff involvement with indecent materials, it would be sensible for the school to seek legal advice as soon as possible, particularly with regard to the disciplinary actions that are acceptable while the police carry out their investigations. Schools should also be prepared for media contact, and have strategies in place for dealing with this.

Conduct an E-Safety Review

In the event of a very serious incident occurring within school, it is essential that a review of all e-safety policies and procedures is conducted as soon as possible. The head teacher would have ultimate responsibility for the review process, but would probably delegate this to the e-safety co-ordinator and the school's e-safety team.

The key components of a safe technological learning environment (based on the PIES model of policy, infrastructure and education, underpinned by standards and inspection) should also be reviewed, ensuring that:

- Comprehensive debriefing occurs after the incident to maximise what can be learnt.
- The network manager has the professional skills to carry out regular safety checks, and knows the correct protocols to follow if illegal material is suspected or encountered.
- All school staff understand the circumstances under which a forensic audit of computers should be carried out, and by whom, and the appropriate strategies to adopt to ensure that evidence is secured and preserved.
- The school's e-safety team contains staff with relevant expertise, and that the appropriate time and authority is allocated to the team to allow them to carry out their duties effectively.

What Illegal Content can be Reported?

You should make a report to the Internet Watch Foundation anything that you believe to be potentially illegal:

- Images of child abuse hosted anywhere in the world. As a guide, the word 'indecent' means any images of children, under 18 years of age, involved in a sexual pose or activity. The term child abuse images reflect the gravity of the images but they are also commonly referred to as child pornography, child porn, child porno and kiddie porn.
- Criminally obscene content hosted in the UK. As a guide it could include images featuring acts of extreme sexual activity such as bestiality, necrophilia, rape or torture.
- Incitement to racial hatred content hosted in the UK. The law on incitement to racial hatred content makes it an offence to stir up racial hatred against a group of persons in Great Britain, defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.

If you are unsure as to whether the content is legal or not, be on the safe side and report it.

Source: www.becta.org

5.1.2 - SAMPLE ACCEPTABLE USE POLICY

Below is a template for an Acceptable Use Policy. Generic terms such as youth service, young person/people or youth worker can be replaced with whatever is most suitable or appropriate to your setting.

SAMPLE ACCEPTABLE USE POLICY

Youth Service Name: _____

Address: _____

The aim of this Acceptable Use Policy is to ensure that young people who use the service will benefit from learning opportunities offered by the Youth Service's Internet resources in a safe and effective manner. Internet use and access is considered a resource and privilege. Therefore, if the AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

It is envisaged that the Youth Service and parent representatives will revise the AUP annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

This version of the AUP was created on _____ (date)
by _____ (name of parties involved in drawing up the AUP)

Youth Service's Strategy

The Youth Service employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a youth worker.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The Youth Service will regularly monitor young peoples' Internet usage.
- Young people and youth workers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal floppy disks, memory sticks, CD-ROMs, or other digital storage media in the Youth Service requires a youth worker's permission.
- Young people will treat others with respect at all times and will not undertake any actions that may bring the Youth Service into disrepute.

World Wide Web

- Young People will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Young People will report accidental accessing of inappropriate materials in accordance with Youth Service Procedure

- Young People will use the Internet for educational purposes only.
- Young People will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Young People will never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies, is in direct breach of the Youth Service's acceptable use policy.
- Young People will be aware that any usage, including distributing or receiving information, Youth Service-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

- Young People will use approved email accounts under supervision by or permission from a youth worker.
- Young People will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Young People will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Young People will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Young People will note that sending and receiving email attachments is subject to permission from their youth worker.

Internet Chat

- Young People will only have access to chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the Youth Service.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

Youth Service Website

- Young People will be given the opportunity to publish projects, artwork or Youth Service work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the Youth Service's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of any young person or member of staff/volunteer.
- Website using facilities such as guestbooks, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details.
- The publication of work by a young person will be co-ordinated by a youth worker.
- Work by a young person will only appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The Youth Service will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the Youth Service website without the parental/guardian permission. Video clips may be password protected.
- Personal information on a young person including home address and contact details will be omitted from the Youth Service's web pages.

- The Youth Service website will avoid publishing the first name and last name of individuals in a photograph.
- The Youth Service will ensure that the image files are appropriately named – will not use young people’s names in image file names or ALT tags if published on the web.
Young people will continue to own the copyright on any work published.

Personal Devices

Young People using their own technology in the Youth Service i.e. sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the Youth Service’s acceptable use policy.

Legislation

The Youth Service will provide information on legislation relating to use of the Internet which staff, volunteers, young people and parents should familiarise themselves with.

Support Structures

The Youth Service will inform young people and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including withdrawal of access privileges and, in extreme cases, suspension or expulsion from the Youth Service. The Youth Service also reserves the right to report any illegal activities to the appropriate authorities.

Permission Form Template

Please review the attached Youth Service Internet Acceptable Use Policy, sign and return this permission form to the Youth Worker.

Youth Service Name: _____ **Name of Young Person:** _____

Young Person

I agree to follow the Youth Service’s Acceptable Use Policy on the use of the Internet. I will use the Internet in a responsible way and obey all the rules explained to me by the Youth Service.

Young Person’s Signature: _____ **Date:** _____

Parent/Guardian

As the parent or legal guardian of the above young person, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the Youth Service to provide for online safety but the Youth Service cannot be held responsible if young people access unsuitable websites.

I accept the above paragraph

(Please tick as appropriate)

I do not accept the above paragraph

In relation to the Youth Service website, I accept that, if the Youth Service considers it appropriate, my child's work may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing children's work on the Youth Service website.

I accept the above paragraph

(Please tick as appropriate)

I do not accept the above paragraph

Parent/Guardian Signature: _____ **Date:** _____

Address: _____

Telephone: _____

5.2 RESOURCES

5.2.1. IRISH CONTACT AGENCIES

Office for Internet Safety

The Office for Internet Safety has been established by the Government to take a lead responsibility for internet safety in Ireland, particularly as it relates to children, under the aegis of the Department of Justice, Equality and Law Reform

Office for Internet Safety

Floor 3, Block 2, Harcourt Centre, Harcourt Street, Dublin 2

Tel: 01 4086122

Email: internetsafety@justice.ie Web: www.internetsafety.ie

Irish Internet Association

The Irish Internet Association is the professional body for those conducting business via the internet from Ireland.

Irish Internet Association, The Digital Hub, 101 James Street, Dublin 8 Tel: 01 5424154

Email: info@iia.ie Web: www.iia.ie

ISPAI www.hotline.ie Service

The Internet Service Providers Association of Ireland aims to provide one voice for the Irish ISP industry at national, EU and International level. The Association is represented at many government initiatives and provides a public point of contact for the media. It established the www.hotline.ie service to combat illegal content, especially child pornography, being hosted and distributed on the Internet.

ISPAI www.hotline.ie Service

Unit 24 Sandyford Office Park, Dublin 18

Tel: 1890 610710 Fax: 01 294 5282

Email: info@Hotline.ie Web: www.hotline.ie

NCTE

National Centre for Technology in Education is an Irish Government agency established to provide advice, support and information on the use of information and communications technology (ICT) in education.

NCTE, Dublin City University, Dublin 9

Tel 01 7008200 Fax: 017008210

Email: info@ncte.ie Web: www.ncte.ie

Webwise

Webwise is the Irish Internet Safety Awareness Node managed by the NCTE. Webwise provides parents, teachers, and children with educational resources, advice and information about potential dangers on the Internet and empowers users to minimise or avoid these risks.

Web: www.webwise.ie

5.2.2 USEFUL IRISH WEB-BASED RESOURCES

<http://groups.google.ie/group/social-media-and-youth-work> has a wide range of resources available to be downloaded including the following:

Exploring Bebo a Starter Guide for Youth Workers - step by step tutorial on how to use bebo for youth workers
SurfwisE Educational Programme for Teachers - manual for teachers from Webwise focuses on internet use in general and not social networking and social media in particular

Webwise 10 Tips for Parents - list of dos and don'ts for parents focuses on internet use in general and not social networking and social media in particular

Webwise Get With It: Parents Guide to Social Networking - in-depth exploration of safety and social networking for parents in simple and easy to use language

Webwise Personal Information Poster - Awareness poster for young people to illustrate the dangers of posting photos of oneself

Cyberbullying Poster - poster providing info to young people on how to respond to text/cyberbullying

www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-en

www.internetsafety.ie/website/ois/oisweb.nsf/page/publications-en

These two sections within the Office for Internet Safety website contain a range of downloadable documents on safe Internet use for both parents and children; safe use of mobile phones; social networking; protecting children online and cyberbullying.

Watchyourspace

Website aimed at raising awareness of Internet safety issues and promotes safe, responsible practice by young people when online. It is part of the NCTE's Webwise Internet safety initiative targeted at teenagers and young adults. The site is divided into 6 main areas containing clearly presented safety messages including a series of video clips of interviews with young expert using social networking sites, mobile phones and the Internet in general. It covers practical information and advice on a selection of online activities such as dealing with and reporting serious issues, online publishing and uploading images.

www.watchyourspace.ie

Webwise

Invaluable website which contains an extensive range of downloadable resources and publications, learning tools and a series of online training sessions with worksheets, handouts and posters for working with young people on different aspects of safe Internet use.

www.webwise.ie

Selected International Safe Internet Use Resource Websites

In addition to the safety information included in these guidelines much of it from social networking sites there are a multitude of excellent safety resources available online from many dedicated websites. Listed below are just a few of them:

www.connectsafely.org

www.cyberbully.org

www.haltabuse.org

www.kidsmart.org

www.netsmartz.org

www.safekids.com

www.wiredsafety.org

www.youngpeoplesafeonline.org

5.3 RELEVANT LEGISLATION

In general there is limited legislation in Ireland relating to the use of IT and the Internet. Anyone who is familiar with Internet use will be aware of how difficult it is to regulate its use, what appears on it and inappropriate use of it. There is also an ongoing philosophical debate as to whether people should be trying to regulate it as many argue that it is the one true uncensored forum for individuals in the modern world and therefore should be protected as such.

However, there are a number of pieces of legislation, while not specifically focused on IT and the Internet, do have provisions within them that are relevant.

Criminal Law (Sexual Offences) (Amendment) Act 2007

This Act introduced an offence of meeting a child or travelling to meet a child, having “groomed” the child on at least two previous occasions, for the purpose of doing anything that would constitute the sexual exploiting of the child. The maximum penalty on conviction on indictment is imprisonment for a term not exceeding 14 years

Non-Fatal Offences Against the Person Act (1997)

Stalking through electronic or physical means carries a penalty of up to seven years imprisonment in Ireland. Also, if an individual continually sends email to someone that is unwanted, explicit, etc. it can be regarded as a harassment offence under section 10 of the Non-Fatal Offences Against the Person Act (1997).

Child Trafficking and Pornography Act 1998

This Act, which is amended by **Section 6 of the Criminal Law (Sexual Offences) (Amendment) Act 2007**, deals with a number of offences involving children under the age of 17 which could be facilitated by use of the Internet. These include:

- Child trafficking and taking a child for sexual exploitation; the maximum penalty is life imprisonment.
- Meeting a child for the purpose of sexual exploitation; the maximum penalty is 14 years imprisonment.
- Allowing a child to be used for child pornography; the maximum penalty is a fine of up to 31,000 euro and/or 14 years imprisonment.
- Producing, distributing, printing or publishing child pornography; the maximum penalty for a summary offence is 1,900 euro and/or a year's imprisonment; if charged on indictment, the maximum penalty is an unlimited fine and/or 14 years imprisonment.
- Possession of child pornography; the maximum penalty for a summary offence is 1,900 euro and/or a year's imprisonment; if charged on indictment, the maximum penalty is 6,350 euro and/or five years imprisonment.

Bibliography of Reference Sources

National Youth Federation, (2003), *Safe Surfing: Guidelines for Safe Internet Use for Young People and Those Who Work With Them*, (Dublin: Irish Youth Work Press)

Byron, T., (2008) *Safer Children in a Digital World: The Report of the Byron Review*, (Crown Copyright: London)

Youth Work Ireland, (2009), *Safe Surfing: Guidelines for Safe Internet Use for Young People and Those Who Work With Them*, (Dublin: Irish Youth Work Press)

Source Websites

<http://ie.playstation.com/>

www.becta.org

www.bebo.com

www.electronicarts.ie

www.facebook.com

www.internetsafety.ie

www.myspace.com

www.secondlife.com

www.teensecondlife.com

www.webwise.ie

www.wiredsafety.org

www.youtube.com

www.xbox.com



Published by the Irish Youthwork Press
20 Lower Dominick Street, Dublin 1.

ISBN: 978 1 900416 69 6

© Youth Work Ireland, 2009