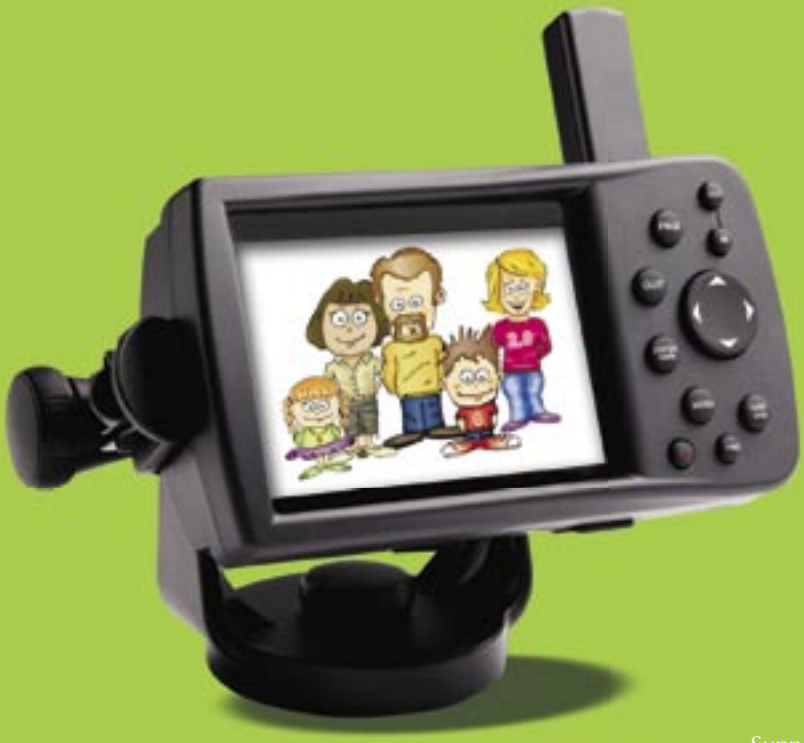
Parental guide

Keeping your children safe online!



Supported by:

webwise.ie

ins@fe

chorus ntl:
a UPC company

SUMMARY

A. How to use this kit

If you plan for one year, plant rice.
If you plan for ten years, plant a tree.
If you plan for a lifetime, educate your child

Chinese proverb

Dear Parent/Carer,

You are holding the e-safety kit for families with children aged between 6 and 12 years. It is an educational resource that was created in the firm belief that new technologies should not separate generations, but unite them. It has been built through the expertise of Insafe, the pan-European network of national contact centres that work to raise awareness on internet safety issues. The development and production of this e-safety kit has been supported by UPC.

Just as playing in the playground or crossing the street can be dangerous if you are not careful, using the internet and mobile technologies also involves dangers for the unwary. Fortunately, there are tools available to empower internet users with knowledge about the benefits, and risks, of surfing the web.

Use your new kit to support your children in learning how to use the internet safely and efficiently. The kit offers over fifty safety tips and exercises to help you teach your children e-safety in a fun, engaging and non-threatening manner. In includes:

- Two e-safety booklets: a family fun section and a parental guide;
- Golden rules;
- A family certificate;
- A set of stickers;
- 12 cut-out situation cards.

Both the family and parental booklets are colour–coded to highlight four key e-safety themes: Security, Communication, Entertainment & Downloading and Cyberbullying. The parental booklet serves as a reference to the family fun section: it contains background information, notes on the activities, and proposed solutions to the exercises and situation cards.

The family booklet is intended to be used by parents and children together. The four themes are approached through the story of two youngsters, Alex and Anna, their parents, and the IT genius, Hedvig. Each chapter contains educational activities, including online exercises, quizzes, golden rules and useful links.

Read the story aloud with your children and together work through the proposed activities. At the end of each chapter, you can use the corresponding situation cards to spark discussion with your children to further enhance understanding of the content.

When your children have successfully worked their way to the end of the toolkit, reward them by agreeing on a set of golden rules and having everyone sign the family certificate. Finally, children can decorate the booklets with emoticon stickers.

Your feedback is valuable to us. Please do not hesitate to contact your local Insafe centre for questions or comments. We wish you and your family the best of fun in taming the internet!

Safe surfing,

webwise.ie

1. Security brings Safety

A COMPUTER @ HOME

A computer at home can be a great educational and recreational resource for the entire family. Placing the computer in a family room in the house and setting specific rules regarding the conditions and time to be spent in front of the screen helps your young family members stay safe.

Remember that your children can access the **internet** at friends' places, at internet cafés, etc. That is why it is important that together you establish a safe and secure code of conduct that they can apply anytime, anywhere.

SECURING YOUR COMPUTER

Security can be achieved through a basic understanding of potential threats and a knowl-

edge of simple remedies. These remedies include useful technological tools and also users' common sense. Like everything else, common sense develops with age and practice.

Things that you and your children are most likely to do on your home computer such as using **memory sticks** or **CD-ROMS**, opening **attachments** and **downloading files** can involve risks. These risks mainly concern malicious **computer programs** (**malware**), designed to harm your computer, steal personal data, or provide you with unsolicited publicity.

Children are introduced to types of malware: **viruses**, **worms**, **Trojan horses** and **spyware** and are taught to recognise the symptoms of an infected computer. They learn how to prevent an infection by always accessing the internet on a computer that is protected by up-to-date anti-virus and **anti-spyware** programs. They are also advised to be careful when opening email attachments from unknown senders, downloading programs from the internet, and using USB sticks or CD-ROMs.

FIGHT SPAM

80% of emails circulating on the internet are **spam** (unsolicited email) that can easily affect your children. Inadvertently publishing an **email address** on the **web** when using a **newsgroup**, **chat** site, a **public forum**, a **social networking** site or an **online form** can generate spam. Specific software can collect email addresses from the web to compose mailing lists that are then used to distribute spam in huge numbers. The companies involved in such activities are often located in places where there is no legislation to prevent unsolicited email!

Spam emails are most often related to pornography, pharmaceuticals, dubious financial transactions, etc. Moreover, spam can also be the source of malicious programs. In most cases, spam emails are distributed with fraudulent intentions. Below are some tips to help you protect your family:

- Use "**spam filters**". Your email provider usually offers anti-spam options that you can activate in your email program. Contact your email provider for detailed information. Regularly check your **junk** or **spam folder** to see if innocent emails have not ended up there. Technology is not fool-proof.
- Teach your children not to open email from unknown people. Spam almost always contains inviting offers and attachments. Show them how to block the sender of an email or just ask them to delete suspicious emails.

SURFING ON THE NET

Even very young children can benefit from surfing the internet for fun and visiting educational **websites**. However, the internet also offers all kinds of content that is not always age-appropriate.

Search engines are great for locating content on the internet. Yet, because searching depends on a choice of keywords, it also makes it easy to locate unwanted content. An inno-

cent sounding keyword could return a not so innocent website containing the keyword in question. Below are some tips for helping your children surf more safely on the internet:

- Create a special user account for your child using an **operating system,** eg. Windows, Linux, Mac OS, on which you can activate **parental controls**;
- Examine the parental control features on your **internet browser** and search engine. Make sure you know the choices offered by the **family settings** of these tools;
- Propose child-friendly **search engines** for the young internet users under your care. An example is *http://kids.yahoo.com*, *http://www.askforkids.com*;
- Save the addresses of the websites your children use the most in their **favourite's** folders (a browser option). In that way you can allow them to use their favourite **net** places again and again without having to pass through a search engine.

As well as activating the parental control features on your browser and search engine, you can use an additional **filter**, software aimed at shielding minors from unsuitable content on the web. Ask for advice from your retailer, or look on the internet for trial **software**. Remember that nothing can replace the guidance of parents and child carers. Technical tools are not fool-proof and can sometimes create a false sense of security unless used in conjunction with your common sense.

Filtering software can be so restrictive that it can block innocent content. It could block children from researching a history essay on the Second World War, for example, because the search leads to websites describing violence. Moreover, any filter that can be switched on, can be switched off by smart youngsters who are often expert in covering their tracks. You will only find out this is happening if you learn how to use the computer and the software yourself.

Visit the website of **SIP-Bench** (see Useful links), a European Commission-supported study under which 30 parental control and anti-spam tools were tested to measure their effectiveness in protecting children aged between 6 and 16 against harmful content in various internet applications: **browsing**, emailing, **file transferring**, chatting and **instant messaging**.

As well as avoiding **harmful content**, you should ensure that your children do not believe everything they see or read on the internet. In the family fun booklet we suggest that they always visit at least 3 websites in order to compare content when looking up information online. They are also advised to systematically mention the source of the information found whenever they use it for a school assignment.

GOLDEN RULES FOR PARENTS OF SURFING CHILDREN

- Ensure your computer is protected by a firewall as well as by antivirus and anti-spyware software. Keep the latter up-to-date and pay attention to any alerts they generate. Check if your Internet Service Provider (ISP) offers antivirus and spyware tools you can use;

• Use a spam-filter on your email program and keep your email address as private as possible, by not publishing it on the web. Avoid emails from unknown senders and scan attachments before opening them;

• Maximise the parental control features of your software on your: operating system, internet browser, search engine and email program. Create separate user accounts for your children. Ensure that privacy settings are at the highest level (visit the "options" menu in your browser);

• Consider using supplementary filtering software;

• Contact an expert as soon as your computer starts behaving strangely, it may be infected. Your ISP should also be able to provide guidance for parents;

• Submit a report to your national internet hotline (see Useful links) if you come across unwanted content online;

• Sit next to your children whenever you can while they are surfing. It is an excellent way of stimulating discussion and increasing trust. Make it a challenge to learn together;

• Remember, these security rules apply to both you and your children. Encourage them to tell you about anything they think looks strange.

USEFUL LINKS

Your kids can take a course on e-safety and follow the Webwise online adventures of Niamh and Fionn:
http://www.webwise.ie/index.aspx

To enjoy surfing safely, knowledge is key: know the risks, know how to protect yourself and know more. More details can be found on the makeITsecure website:
http://www.makeitsecure.ie

Should you stumble across content that you believe may be illegal while surfing on the net, you can submit a report to the Irish hotline service:
http://www.hotline.ie

SIP-Bench:
http://www.sip-bench.org

2. Communicating

PIECES OF THE PUZZLE

Remember how important it was for you to keep in contact with your friends when you were growing up? The internet provides lots of new places to meet friends and offers new ways of self-expression and socialising through emailing, file sharing, blogging, and social networking (e.g. MySpace, Facebook, Hi5, Habbohotel) etc. Teenagers today use technology to try new things and socialise in a space they feel is private and free from parental surveillance.

The communication chapter introduces parents and children to the concept of **personal data**, **privacy**, positive online interactions and managing risks such as contact with strangers. Privacy online is very closely linked to the concept of **accounts** & **profiles**. An account is what makes it possible to access an online service.

Offline, a bus pass, gym card or membership card contains personal information about you. Online accounts and services are similar. You cannot open either unless you provide some personal information that is used to make up your "user profile". Importantly you can choose both the kind of information you want to make available about yourself, and who you want to share this information with.

Protecting your privacy is about managing what you want people to know about yourself rather than lying about who you are. Young people are enthusiastic about communicating with friends online and creating their online image. However, they do not always realise the impact it can have on them when they make their private information public.

CREATING A PROFILE

The first step in protecting personal information is to create a safer profile by thinking carefully about the data it will include and the privacy settings to apply.

Create several email accounts for different online contexts. For example, when using online services such as chat, instant messaging, blogging, etc. encourage your child to use a neutral email address and **screen name**. This way your chatting child is not using an email address that gives out his/her full name.

Always keep account **passwords** secret. Make sure your children understand that they should not share their personal accounts with friends who may misuse their trust. On the other hand, you may want to know your children's passwords so that you can monitor their accounts - talk to them about this.

Remember to customise the **privacy settings** of your profile/account by choosing it to be private and not public. This gives you the opportunity to control who it is visible to and who you can interact with. A private profile means that you can manage your **contact list**. Teach your children to only accept contacts from people they already know from an offline context.

If your children are using chat-rooms check that:

- there are live **moderators** present. No moderator means unsafe chatting;
- there are tools to ignore or block unwanted chatters;
- there is a help and **report** function on the website where they can go in case of problems;
- the rules of the service are clearly and visibly set out.

PICTURES AND WEBCAMS

Children must understand that their photo is an integral part of their privacy and that digital images are extremely powerful. They are easy to circulate and **manipulate**, and very difficult to erase once they've been sent through a computer or a mobile phone - they could stay online forever! Webcams should be used carefully and children should not use webcams without supervision. **Webcam** chat tools and **directories** can be risky. You and your children should only share your personal images with people you know and trust – always get permission before you publish a photo of someone else. Do not let your children use a computer and webcam alone in their room.

CONTACT WITH STRANGERS

People you meet online are not always who they say they are. Teach your children to safeguard their privacy online just as they would offline. You lay down rules about how they behave with strangers in the real world, so why shouldn't they follow the same rules on the internet?

Your children may build a strong relationship with online friends and tend to easily trust people that show interest and understanding for them even if they do not really know them. Consequently, they can be very tempted to meet these new friends offline without informing you. Children are often unaware of the danger of such meetings and may consider them trivial. This makes them easy victims of online **grooming**. Studies show that a lot of children go to meet online "friends" unaccompanied and without telling their parents. Talk to your children about this to make sure it doesn't happen to them. Communication is key.

NETIQUETTE

Netiquette refers to good manners on the internet and treating other people on the net as you would like to be treated yourself. Children may not realise that they can accidentally offend someone online. Unfortunately, some people use the internet and/or mobile phones to upset or harass others. This is called cyberbullying and can affect up to one in four children (see the relevant chapter for more information).

CHAT LANGUAGE

When chatting online young people use a unique language, full of **emoticons** and **acronyms**! Take a look at the tables below to get familiar

Indicative list of chat **acronyms**, for more information see useful links:

121: one to one

AFK: away from keyboard

A/S/L: age, sex, location (or just "ASL")

BBB: bye bye baby

B4N: bye for now

BBL: be back later

BF: boyfriend or best friend

BFF: best friends forever

C: see?

Comp: computer

CU: see you

CUL: see you later

CYO: see you online

EGBOK: everything going to be ok

F2F: face to face

JJ: just joking

K: all right /ok

KFY/K4Y: kiss for you

KISS: keep it simple, stupid

KPC: keeping parents clueless

L8R: later

IRL: in real life

LMIRL: let's meet in real life

LOL: laughing out loud, lots of love

LY4E: love you forever

NE1: anyone

NP: no problem/ noisy parents

OIC: oh, I see

OLL: online love

PAL: parents are listening

G2G or GTG: got to go

<G>: grin

GFN: gone for now

GL: good luck

GM: good morning /good match

HAND: have a nice day

^5: High 5

H2G: have to go

HDOP: help delete online predators

IDK: I don't know

ILU/ILY: I love you / I like you

PAW: parents are watching

PIR: parent in room / people in room

POS: parent over shoulder

RL: real life

S^, S'UP: what's up?

TTYL: talk to you later

TY: thank you

WB: welcome back/ write back

WDYT: what do you think

WTGP: want to go private?

WYCM: will you call me?

You can create emoticons, by combining punctuation marks and letters, see examples below:

A smiley (with or without nose)	**:)** or **: -)** colon, (dash), bracket
A sad face (with or without nose)	**:(** or **:-(** colon, (dash), bracket
Blinking face (with or without nose)	**;)** or **;-)** colon, (dash), bracket
Surprised face (with or without nose)	**: o** or **:-o** colon, (dash), small o
Big smile (with or without nose)	**:-D** or **: D** colon, (dash), capital D
Tongue out (with or without nose)	**: p** or **:-p** colon, (dash), small p

GOLDEN RULES

• Take time to discover how your children spend their time online and let them show you how they communicate with their friends;

• Teach them to safeguard their privacy online by:

- Creating safe profiles with enabled privacy settings
- Protecting their passwords
- Only contacting and replying to people they know offline
- Always asking for parental consent before uploading pictures of themselves or of your family, house, their school etc
- Only share personal information such as their phone number, address, school, sports team etc with people they know well in real life;

• Place the home computer in a family room so you can monitor their online activities;

• Together, make sure you know:

- How to refuse contacts or block persons from a contact list
- The security and reporting functions that are available on the websites you use

• Build trust by reassuring your children that they can talk to you about their mistakes so you can look for solutions together! Mistakes are part of learning.

USEFUL LINKS

'Watch Your Space' is part of the Webwise internet safety initiative targeted at teenagers and young adults. Its focus is to advise and support young internet users:
http://www.watchyourspace.ie

Think U Know purely for parents:
http://www.thinkuknow.co.uk/parents

Break the chat code by visiting wikiHow:
http://www.wikihow.com/Understand-Chat-Acronyms

Consult the Eurobarometer 2007 report on Safer Internet for Children:
http://ec.europa.eu/information_society/activities/sip/eurobarometer

3. Cyberbullying

AN INCIDENT OF CYBERBULLYING

Communicating via the internet and mobile phones has lots of wonderful advantages. Sadly, it can also be less than wonderful - your children may receive or send messages with content that hurts their feelings or the feelings of others. It is important that you teach your children socially acceptable behaviour - even our own children aren't always angels ;-)

Cyberbullying is the use of new information and communication devices and services to bully, harass or intimidate an individual or group. Email, chat, instant messaging, mobile phone or other digital tools may be used. In virtual game environments, bullies may attack your child's **avatar**, e.g. by shooting at it, stealing virtual possessions or forcing the **avatar** to behave in unwanted ways.

Commonly, children report problems related to the disclosure of private information in public spaces, e.g. posting a private photograph or personal information on a public forum or website. Like **bullying** in the school or the playground, such behaviour is not acceptable and parents, educators and children should be alert and ready to respond. Unlike traditional bullying, cyberbullying can affect the child even when he/she is no longer in the presence of bullies. For example, bullies can send threatening messages to home email accounts and mobile phones at any time of the day or night.

Parents can help promote an environment where bullying is not tolerated - teach your children that being anonymous online does not mean they can act irresponsibly. They need to know their own rights and responsibilities, and how to respect other people's rights.

Always maintain an open dialogue with your children, so that you can talk about any worrying situation. New technologies, such as the internet and mobile phones can provide an excellent opportunity for discussion and offer food for thought!

GOLDEN RULES

- Prevent negative experiences by making sure your children know how to protect their own privacy and will respect other people's privacy;

- Teach your children not to respond to harassing messages;

• Help your children understand what kind of messages and behaviour might make others feel bad, and how to avoid this;

• Make sure they know how to block senders from their contact list;

• Keep track of offensive messages, you may need them as important proof;

• Find out your children's school's anti-bullying strategies. Work together with other parents and teachers to prevent bullying and cyberbullying;

• Stay in touch with your children's environment; get to know their friends, their friends' parents, their teachers and classmates;

• Encourage your children to tell you about any troubling offline & online experience. Reassure them that even if they do something careless, you are there for them and together you will find solutions!

• Be sure your children understand that they are never to blame if someone harasses them.

USEFUL LINKS

On the cool school bully-free website you'll find information that helps people understand more about bullying in schools and how it can be stopped:

http://www.nehb.ie/coolschoolbullyfree/kids1.htm

On the stop bullying website you'll find cartoons about bullying and proposed classroom activities about how to deal with it and how to stop it:

http://www.stopbullying.org

Childline is a 24-hour service for young people up to 18 years of age in Ireland. Childline offers support to young people through the Childline listening service over the phone and through the Childline Online website:

https://www.childline.ie/

Childline Online's toll-free number:

1800 66 66 66

4. Entertainment & Downloading

ALL THAT GLITTERS IS NOT GOLD ON THE INTERNET

The internet is a virtual space for lots of activities, including commercial ones. If you do not let your children have everything they see advertised on TV, or that impresses them in the shops, then you should also teach them not to want or believe everything that is advertised online either, e.g. music and games, **ringtones**, other accessories and buying services online.

Spending time with your children on the internet gives you the opportunity to explain that products such as ringtones, **wall-papers**, **mp3**s, **avatars** etc. are rarely free. Whenever you find such advertisements, show them the small print to demonstrate that they should not take everything on the net for granted.

To subscribe to any service (free or not), you will have to fill in an **online form** with relevant personal information. Only complete these forms when you know how your personal data will be used, and discourage your children from using such forms unless you complete them together.

Pop-up windows are often used to sell things on the internet. They are not always bad - it depends whether they come from a trusted website or not. Generally, if you trust the website you can trust the pop-up. However, some pop-ups are used to market products that are unreliable or lead to online questionnaires collecting personal data. Teach your children to close untrustworthy pop-ups by clicking on the red cross at the top right corner.

PLAYING GAMES ONLINE

Online games differ from older digital games because they require a live **network connection**. Children can play games on a CD/DVD on **websites**, on game consoles or on mobile phones and other handheld devices.

Online games range from simple, well-known games such as Pacman and Tetris to virtual reality games where several users play together online, creating content and stories. Many such **multiplayer games** support virtual communities of players. This can expose children

to risks associated with meeting people they don't know on the internet (see the chapter on Communication).

Games play an important role in children's development as social skills and strategic thinking are developed in an environment bounded by playing rules. Many digital games are attractive and interactive and are used for educational purposes.

However, not all digital games are good quality. You must decide what kinds of games are most suitable for your children - and, by setting rules, you can ensure that the amount of time your children spend playing online is not detrimental to other activities.

There is a pan-European age rating system for interactive games, PEGI online, where games are classified according to age and content. The system is supported by several manufacturers, including PlayStation, Xbox and Nintendo, as well as by publishers and developers of interactive games throughout Europe. Look for these specifications on the back of any game box you buy for a child, but remember, not every 12 year-old is the same.

SHARING FILES & COPYRIGHT ©

Young people see the internet as a treasure trove of films, music and games to download, watch, listen to and play. They often download and upload material using **peer networks** without realising that the original work of artists or other creators/authors is protected by **copyright**. This includes things like films, songs, books, software and pictures.

Is it illegal?

File sharing is not illegal if it involves sharing files containing content that you have created yourself. Generally, uploading and downloading music and films without permission from the rights holder is illegal throughout the world (although each individual country has its own copyright law). As a rule of thumb, consider file sharing of music and films illegal and be careful with **peer-to-peer** applications.

Is it risky?

File sharing puts your computer at risk by opening ports through which malicious programs and malware can enter, leading to the computer not functioning properly. It's also possible that other people could access your personal data or use your computer for sending spam or **illegal content**.

Where can I find legal music?

Hundreds of websites worldwide offer music for sale legally (see Useful links), and sometimes even for free! Examples are websites where musicians want fans to sample their work and learn about concerts and albums they're promoting.

GOLDEN RULES

- Make sure you use a legal site to download music and films from the internet;
- Encourage your children to use websites offering legitimate content and explain that everything is not what it seems on the net;
- Explain the risks of downloading material from the net without caution;
- Ensure your computer is protected and always use an updated anti-virus;
- Teach your children to save legitimate downloaded files on the hard-disk and scan before opening;
- Always read the privacy statement and the user agreements before you install something. Check (on the internet) if the software you want to download is trustworthy;
- Close untrustworthy pop-up windows by clicking on the red cross at the top right corner. Never click inside them.

CHILDREN & GAMES:

- Set out rules regarding the amount of time your child can play;
- Let them play in a family room where you can keep an eye on them;
- Monitor your kids' playing habits - if you watch over them in the playground, why not do the same when they play in virtual places?
- Discuss the content of the game, which features are reality-like and which are not, what do they enjoy?
- Before you buy any game for your child, make sure you know that the content is age appropriate (pan European PEGI system or any national rating system).

When your kids play online games with multiple users:

- Choose sites with strict rules and live moderators;
- Warn them not to give out personal details to other players;
- Warn them not to meet other players offline unless accompanied by you;
- Encourage your children to report bullying, threatening or bad language, the display of unpleasant content, or invitations to meet outside the game;
- Withdraw your child from the game or change your child's online ID if anything within the game or the way it evolves makes you feel uncomfortable.

USEFUL LINKS

Learn more about online games and the PEGI age-rating system:
http://www.pegioline.eu

A list of worldwide websites where you can buy music legally:
http://www.pro-music.org

Webwise offers good tools for becoming chatwise, sharewise and gamewise. Explore the interactive lessons with your children:
http://www.webwise.ie/index.aspx

Make sense of TXT lingo on the transl8it website:
http://www.transl8it.com

Get smarter on net "lingo" by visiting:
http://www.netlingo.com

1. Security brings Safety

ANNOTATED ACTIVITIES

Match the picture with the words: Computer tower, mouse-pad, screen, loudspeakers, **web-cam**, printer, USB stick (or memory stick), mouse, CD-Rom.

A warm-up exercise to acquaint your children with the different parts of the computer and other related hardware. You can build on it as you think is appropriate.

Ask your parents to send you an email with an **attachment**, or send yourself one. Practice the following: right click on the attachment and save it on your computer desktop. Go to your desktop, right-click on the document and click on **scan**. When you know the document is safe you can open it. Remember: Right click and SAVE – SCAN – OPEN.

Send an email to your child's email address or to your own address and attach a file. Let your child follow the instructions in the exercise to save the document by right-clicking on it without opening it. After saving the file on the Desktop or a computer folder such as My Documents, show your child how to right-click once more on the document to scan it before opening it to encourage safe habits.

Follow Helen's advice and learn how to describe your email address whenever you really need to publish it online. This is to avoid having your email picked-up automatically and used by spammers. Example: cybercat.smith@mymail.com = cybercat dot smith at mymail dot com
To practice, describe the email addresses you have in the family: *your email, your family email, your mother's email, your father's email*

To avoid having your public email automatically picked up by software for spam distribution purposes, describe it rather than writing it as is. Let your child practice this technique as suggested above. Bear in mind however, that your children should refrain from publishing their email on the internet, and if they do so, they should use one that does not revealing their name (see chapter Communicating).

To help Anna understand before Helen goes any further, take a look at the activities in the box and draw a circle around those things that you can only do if you're connected to the internet.

Your very young children may not be exactly clear about which activity requires a network connection and which does not. Writing a text does not require a connected PC, but chatting does. You can listen to music on your PC by using a CD or a music file that is stored on your computer, but you can also directly listen to music online. Your children should mark only those activities for which a network connection is essential.

Together with your parents type http://kids.yahoo.com in your browser. Look up information on Tyrannosaurus Rex, and try to discover when this dinosaur lived on earth. Also try to find a good picture representing a Tyrannosaurus. Do not forget to cross-check on three different websites.

Teach your children good searching habits by reminding them not to trust everything they see online. Remind them to search and compare information on at least three sites and always state their sources when writing a school assignment.

Together with your parents type http://kids.yahoo.com in your browser. Then search for a subject, for example Tyrannosaurus Rex, and save the three sites you think are most interesting by clicking on the favourites menu at the top of the browser page and adding them to your favourite sites. You can make your own folder too.

Saving and organising interesting sites in the favourites folder (browser toolbar option) is a very good way of reducing the need for your young children to look up information on the internet.

DID YOU GET IT RIGHT?

1: (protected) 2: (virus),(unknown), (downloading), (infected),(memory stick), (unprotected) 3: (strangely) 4: (know),(attachments), (subjects), (spam) 5: (single), (spam) 6: (first), (three), (compare),(anyone), (publish) 7: (anti-virus), (anti-spyware) 8: (talk), (parents) 9: (tell)

SUGGESTED SOLUTIONS TO SITUATION CARDS

SITUATION 1. Never surf the internet if your computer is not protected by an updated anti-virus and anti-spyware programme. It's like having a border with no border guards; your computer could be infected by harmful programmes, such as viruses, Trojan horses, worms or spyware.

SITUATION 2. Keep your eyes open for emails that come from people you do not know and contain attachments or emails that 'promise the world' - they are most probably spam! Spam can infect your computer with harmful programmes, such as viruses, Trojan horses, worms or spyware. Do not open these emails. Instead, block the sender by right-clicking on the email and selecting 'Block sender' or else simply delete them.

SITUATION 3. When you research information on the internet, don't immediately trust the first good page you get. Check at least three different sites and compare the information you find on them. Remember: anyone with internet access can create and publish information on the net. When you write a report or assignment, you must always mention the source of the information and pictures you have used… that's what a true scientist would do.

2. Communicating

ANNOTATED ACTIVITIES

Mark how **private** the following are to you: Your telephone number, Your hair colour, Your name, The country you live in, The school you attend, Your address, The name of your pet, Your parents' professions, Your email address, Your pictures, Your age.

Do your children have the same perception of privacy as you? The three colours represent very private (red), quite private (orange) and not so private (green) information.

Help Anna create a really good password by following Helen's tips.

Good passwords should contain a random set of different characters (numbers, letters and punctuation marks) and should always be kept secret.

Follow Anna's example and create a safe profile. Then make an example of an unsafe one.

Let your children create a safe profile and then a less safe one which discloses private information. Remind your children that creating a safe profile does not protect them if they do not continue protecting their privacy when communicating online.

Review this picture and write down what you can tell about this person.

What personal information can one deduce from a picture? Children are often unaware of the power of images.

Follow Anna's idea and think of 3 pieces of advice "Alex Red Sweater Hood" would get from Helen for protecting himself against "web-wolves"?

Check if your children have realised that contacting strangers online can entail risks.

How would you like people to treat you online? (1….. 2….. 3…..)

Make sure your children understand that they should treat others as they wish to be treated themselves…

BREAK THE CODE: Discover what some of the most popular chat acronyms mean by connecting them to their meaning.

Improve your understanding of acronyms by consulting the chapter Communicating / Netiquette, chat language.

Use keyboard combinations to symbolise these emoticons: A smiley - A sad face - Blinking face - Surprised face -Big smile - Tongue out.

See the chapter Communicating / Netiquette, chat language for more information.

DID YOU GET IT RIGHT?

1: (profile) 2: (privacy), (responsible) 3: (strangers), (tell) 4: (Netiquette), (treated) 5: (emoticon) 6: (password), (punctuation) 7: (secret) 8: (refuse) 9: (know)

SUGGESTED SOLUTIONS TO SITUATION CARDS

SITUATION 4. When you use the internet, your profile, or the information you give about yourself, can reach tens, hundreds, thousands or even millions of people. That is why it is important to carefully choose the information you give away about yourself. Only give personal information to people you trust and know well offline.

SITUATION 5. Mike probably shared his email password with his friend who then decided to get back at him by sending nasty emails on his behalf. Always keep passwords to yourself unless you have nothing against other people reading your emails or pretending they are you and saying things that you would never say!

SITUATION 6. Meeting a stranger is not a very good idea. But if you really think you can trust an online friend who wants to meet you, tell your parents about it and make sure one of them accompanies you. No real friend with honest intentions would have a problem with that. It's only a problem for people who have something to hide.

3. Cyberbullying

ANNOTATED ACTIVITIES

Draw a picture of the invitation Alex received from his teachers. Show the anti-bullying logo and slogan the school is using for the anti-bullying week.

Let your children be creative and draw in the empty frame.

Follow Alex's example and give five reasons that would make you give a "red card" to someone.

Discuss with your children what kind of behaviour they find unacceptable.

DID YOU GET IT RIGHT?

1: (fair), (spoil) 2: (talking) 3: (good) 4: (cyberbullying) 5: (block) 6: (know) 7: (answer)

SUGGESTED SOLUTIONS TO SITUATION CARDS

SITUATION 7. This is definitively not an acceptable way of using your mobile phone. Do not circulate messages, pictures or other material that can be hurtful. Always treat others as you would want to be treated yourself. In such a situation, always talk to your parents or another adult that you trust.

SITUATION 8. Alex should tell his friend that the bad behaviour of the bully is not his fault. He should not respond to the messages from the bully, but keep them as proof and show them to his parents or teachers. Alex should also talk about this to his parents who can support him in helping his friend.

SITUATION 9. Netiquette is about treating others on the web as you would want to be treated yourself. We are sure you have learned enough by now to help Anna in this task.

4. Entertainment & Downloading

ANNOTATED ACTIVITIES

Open your favourite search engine. Type in "free ringtones" or "free games", and see what you get. **Check a few websites. Can you find any traps?**

Practice by making a search with the given keywords and check the websites you find for marketing traps. See how the information in small print is omitted in the advertising slogans.

What is your favourite computer game? Check if your parents know it and can describe it. If they have no clue, explain first, and then let them write a small description. Did they get it right? How many points do you give them out of ten? …/10. Parent fills in a summary of child's favourite game, child draws a picture of it.

Do you really know what kind of games your children play online, and do you know which game is their favourite? Let them put your understanding to the test!

DID YOU GET IT RIGHT?

1: (free) 2: (forms) 3: (traps) 4: (illegal) 5: (cross) 6: (ignore) 7: (privacy) 8: (share), (yourself) 9: (download)

SUGGESTED SOLUTIONS TO SITUATION CARDS

SITUATION 10. Most of the music and films you find on the internet are illegal copies. Besides, websites where people share music and films are usually full of harmful programmes, such as viruses, Trojan horses, worms and spyware. The best solution for Anna would be to choose option b or c. Of course, downloading her favourite song from a reputable site with legal music will cost her much less than buying the entire CD. She would have to ask her parents for their opinion and permission.

SITUATION 11. There are free services on the internet, but ringtones, wall-papers, MP3s, avatars and the like are rarely available for free. If Alex takes a closer look at that website, he will probably discover some very small print, telling him about the real cost of the service. Ringtones, quizzes, games, etc., are all excellent ways of luring people into subscribing to so-called 'free' services that will, in reality, cost them money.

SITUATION 12. Alex should remember to keep his identity private whenever he plays online with people that he does not know in real life. He should not give information about where he lives, the school he attends, his last name, etc. He should also inform his parents about the games he is playing and he should never download any game from the internet before asking them, as this could harm the home computer.

D. Glossary

Account: an account allows you to be authenticated and authorised to use online services through a user name and password. You can use your operating system to create separate user accounts for every family member.

Acronym: an abbreviation consisting of the first letters of each word of a phrase or expression. Acronyms are frequently used by chatters to render communication quicker, e.g. LoL, CU, Btw (see chapter communicating).

Alert: a small box appearing on the display screen to give information or to warn about a potentially damaging operation, e.g. new mail or state of play of your anti-virus protection.

Anti-virus: a computer program that attempts to identify, isolate, obstruct and eliminate computer viruses and other malicious software. The anti-virus initially scans the files to look for known viruses and then identifies suspicious behaviour from computer programs that indicate infection.

Anti-spyware: a program that combats spyware. The program scans all incoming data for spyware software and then blocks the threats it finds or provides a list from which to delete suspicious entries.

Attachment: a computer file which is sent along with an email message. Worms and viruses are often distributed as email attachments. Emails from unknown senders with attachments should be considered suspicious.

Author: the creator of a literary or audiovisual work, a software, etc. Copyright protects authors' creations against illegal reproduction.

Avatar: the profile of a user represented by a username plus an image, icon, or a 3D character in online computer games and virtual worlds.

Blog: short version of weblog. A website for which an individual or a group generates content, usually on a daily basis, consisting of texts, pictures, audiovisual files and links.

Blogging: the act of writing or updating your blog.

Browser: a program used for viewing web sites. Internet Explorer, Netscape Navigator and Firefox are some of the most common browsers for Windows, while Safari is common on Macs. Most recent versions of these browsers contain innovative parental control features.

Browsing: the act of using a browser in order to view web sites, or just surfing the net.

Bullying: harassment through repeated harm, threats, sexual remarks, physical assault and pejorative speech perpetrated by one or more bullies.

CD-Rom: an acronym for Compact Disc read-only memory. It is a non recordable Compact Disc with data legible by a computer. CD-ROMs are popularly used to distribute computer software.

Chat: synchronous communication over the internet through written messages, by using chat and instant messenger applications (e.g. MSN).

Chat room: public virtual place for real time communication. People from around the world can meet in chat rooms and discuss through messages they write using the keyboard. If your children use chat rooms, ensure they are specially designed for their age with supervisors and moderators.

Child pornography: In some countries this is referred to as "child abuse imagery" to reinforce that behind images of child pornography there is abuse of real children. Child pornography has different legal definitions in different countries.

Computer file: an archive/collection of related information (documents, programs, etc) stored on a computer under its own filename. Computer files can be considered as the modern counterpart of paper documents which were kept in office and library files.

Computer program: usually referred to as software. Software consists of a structured sequence of instructions written by computer programmers, which enable computers to perform tasks. When you buy a software program, it often comes on a CD-Rom (see definition), a physical means of storing programs.

Contact list: a collection of contacts in instant messaging and email programs, online games, mobile phone, etc. Contacts can be added, rejected and deleted.

Cookies: a file placed on your internet browser by a website. Each time you access the website again, the cookie is sent back to the server on which the website is stored. Cook-

ies report on your site preferences and are used on online shopping facilities. Rejection of cookies can make certain websites unusable.

Copyright: a set of exclusive rights regulating the use of an idea, work or information. Copyright is represented by the symbol "©".

Cracker: a person who illegally breaks into computer systems.

Crack: to illegally copy commercial software by breaking the copyright protection feature.

Cyberbullying: refers to bullying over electronic media, usually through instant messaging and email. It may involve repeated harm, threats, sexual remarks, and pejorative speech. Cyber-bullies may publish personal contact information of victims and even assume their identity and publish material in their name for the purpose of defaming or ridiculing.

Directory: an organisational unit that your computer uses to organise folders and files into a hierarchical structure, e.g. My Documents, My Pictures, etc.

Download: refers to the process of copying a file from an online service to a computer.

Email: a means of electronic written communication that allows you to send messages with any kind of computer file attached - text, pictures, audio and more.

Email address: a virtual location to which email messages can be delivered. Email addresses consist of two parts, separated by the @ symbol.

Emoticon: an image, icon, used to convey feelings and emotions, e.g. smiley. It can be symbolised by using standard keyboard characters and punctuation marks or by using prefabricated characters provided in chat rooms, game rooms, instant messaging services, mobile phones, etc.

Family settings: also known as parental controls. Settings used to customise a browser or other web tool in view of making them more children friendly by the use of features such as content filtering, time limitation, game controls, etc.

Favourites: a customisable browser folder where you can save interesting links/bookmarks. The bookmarks can be organised in sub-folders and/or tagged with keywords for easy search.

File sharing: online exchange of files between computer users. The term covers offering files to other users (uploading) and copying available files from the internet to a computer (downloading). Typically files are shared via P2P (peer-to-peer) networks.

File transfer: the act of transmitting files over a computer network. From the user's perspective, file transferring is often referred to as uploading or downloading.

Filter: application which regulates access to information or specific internet services, warns against problematic websites, keeps track of user's navigation, blocks risky sites and even turns off a computer altogether. Filter systems can be installed on stand-alone computers, servers, phones with internet access, etc.

Firewall: a hardware (integrated in your router) or software (installed on your PC) device configured to prevent unauthorised users (such as hackers and crackers) from accessing a computer or a computer network connected to the internet.

Flaming: a hostile and insulting interaction between internet users. It usually occurs in discussion boards, Internet Relay Chat (IRC) or even through email.

Folder: an entity in a file system which contains a group of files and/or other directories. Folders can contain multiple documents and are used to organise information.

Form (online form): a formatted document containing blank fields that you can fill in with data. The electronic form can be filled in with free text or by choosing alternatives from pre-established lists (drop-downs). After submission, the data is directly sent to a processing application which enters the information into a database.

Forum: an online discussion group where participants with common interests can openly exchange messages on different topics.

Freeware and shareware: in general, software is protected by copyright and can therefore not be downloaded. Freeware means that the copyright holder of the software consents to the software being used by anyone free-of-charge. Shareware means that the copyright holder consents to the software being used by anyone for a trial period. After that period, the user has to pay a fee to keep on using the service.

Digital Game: a game created by game developers and played on a computer. An online game is defined as a digital game that needs a live network connection in order to be played. Online games can support interaction between multiple players.

Grooming: the use of chat rooms by paedophiles to groom children by pretending to be their peers. Paedophiles initiate conversations with likely victims to extract information about location, interests, hobbies and sexual experiences. Predators use various means of attracting children in conversations of sexual nature.

Hacker: popularly used term to refer to a person who engages in computer cracking (see 'cracker'). Can also be used in computing circles to describe a person who is a computer enthusiast.

Hardware: the physical part of a computer, as distinguished from the computer software that executes within the hardware. It can be internal: motherboards, hard drives, and RAM - often referred to as components; or external: monitors, keyboards, printers, etc - also called computer peripherals.

Harmful content: pictures, texts, documents, etc whose content is capable of causing harm, e.g. images depicting violence are unsuitable and damaging for children and minors.

Helpline: an email and sometimes telephone service provided in several countries by child support organisations and Insafe network members. Children can raise concerns about illegal and harmful content and uncomfortable or scary experiences related to their use of online technologies.

Homepage: is the webpage that automatically loads when a web browser starts. The term is also used to refer to the front page or main web page of a website (see definition).

Hotline: telephone support line or web-based service where people can complain about alleged illegal content and/or use of the internet. Hotlines must have effective transparent procedures for dealing with complaints and have the support of government, industry, law enforcement and internet users in the countries of operation.

Identity theft: stealing personal details (e.g. name, birth date, credit card number) and using them illegally.

Illegal content: online content which is illegal under national legislation. The most common types of such content are images of sexual abuse of children, illegal activity in chat rooms (e.g. grooming), online hate and xenophobia websites.

Instant Messaging (IM): a form of instant and simultaneous electronic communication between two or more users. IM allows you to communicate with a selected list of contacts. When people in your contact list are online, you're immediately alerted.

Internet: is a worldwide, publicly accessible network of interconnected computer networks through which data transmission and exchange takes place. It comprises smaller domestic, academic, business and government networks which carry various services such as information, email, online chat, file transfer, etc.

Internet connection: refers to the means by which users connect to the internet. Common methods of internet access include dial-up, T- lines, Wi-Fi, satellite and cell phones.

Junk/Spam folder: in an email box, the place where emails that are considered to be spam or junk are stored.

Junk mail: unwanted, nearly identical email messages that are sent out to people via their email address. As the internet is public, there is really little that can be done to prevent junk email, just as it is impossible to prevent spam.

Link: a reference to a document available online (web page, text document, picture, etc). When you click on the link you get to a new page or a completely different website. Text links are typically blue and underlined, but they can also be any colour and not underlined. Images can also serve as links to other web pages.

Malware: short for malicious software, represents software designed to infiltrate or damage a computer system without the owner's informed consent. It includes computer viruses, worms, Trojan horses, spyware, dishonest adware and other malicious and unwanted software.

Manipulate: the process of altering an image, file, photo, or illustration in an apparent or non apparent way. Nowadays, there are numerous tools that can be used to influence the content or shape of data leading to a result different from reality.

Massively Multiplayer Games: games that offer a rich 3D world populated with thousands of gamers assuming the roles of fictional characters and competing against each other.

Role-playing games are dominant in this category where participants collaboratively create or follow stories.

Memory/USB stick: data storage device integrated with a USB (universal serial bus) connector. A memory stick is typically small, lightweight, removable and rewritable.

Mobile: an electronic telecommunications device, also known as mobile phone, cellphone, gsm, smartphone, handphone. It has the same basic capability as a conventional fixed line telephone. Today most mobiles integrate a camera and many offer access to internet (a paying service).

Mp3: is an audio-specific encoding format. An mp3 file is about one tenth the size of the original audio file, but the sound is nearly of CD-quality. Because of their small size and good fidelity, mp3 files have become a popular way to store music files on both computers and portable devices.

Net: abbreviation for the internet.

Netiquette: internet etiquette dictating civility rules for online communications.

Newsgroup: see definition for forum.

Nickname: a synonym for screen name and handle. It represents the user of an online service and is defined by the user him/herself. It represents users in contact lists, chat rooms, etc. Nicknames, if well chosen, can protect your anonymity online.

Operating system: a program that runs the basic functions of a computer, making it possible for other programs to run. Well-known examples are Windows, Linux and Mac OS.

Parental control: see definition for family settings.

Password: a secret series of characters that enables its owner to access a file, computer, account or program as a safety measure against unauthorized users (see chapter Communicating).

Personal data: any information that can be linked to a person. If personal data has to be collected, processed and stored, the purposes have to be explicitly stated.

Pop-up window: a window that suddenly appears when visiting a website or pressing a special function key. Usually, pop-up windows contain a menu of commands and stay on the screen only until you select one of the commands or close it by clicking on the top-right corner cross.

Port: is an interface on a computer used to connect it to another device. Ports can either be internal or external. Internal ports make a connection to a disk drive or a network, while external ones connect to a peripheral device like a printer or a keyboard.

Privacy: the ability of an individual or group to control the flow of information about themselves and thereby reveal themselves selectively. Privacy is sometimes related to anonymity, the wish to remain unnoticed in the public world.

Privacy setting: a set of account-specific privacy details that you can edit in order to enhance privacy against disclosure of personal information, cookies, etc.

Private: things about an individual or group that are not to be revealed to the public. When something is private to a person, it usually involves something considered inherently special or personally sensitive.

Processor: or Central Processing Unit (CPU) is the part of a computer that processes data, generates control signals and stores results. Together with the computer memory, it forms the central part of a computer.

Profile: personal user information in social networking spaces, instant messaging systems, online chat applications, online games, etc. Profiles can be public or private, are customised by users to represent themselves in virtual places.

P2P network: a peer-to-peer (P2P) network allows those who are connected to it to exchange files by uploading and downloading (see definition). It is only one of several ways files are shared on the internet. Some file sharing services are illegal.

Recycle bin: a computer directory where deleted files are temporarily stored before users permanently delete them. You have to regularly remove old and unwanted data from the recycle bin to free up space on the hard disk, your computer's internal storage.

Report: a function that allows users of public virtual spaces to report a problem (technical, unacceptable user behaviour, illegal content, etc.) to the moderator or webmaster.

Ringtone: a mobile phone sound for incoming calls. There is a large variety of customisable tones and music available for cell phone owners to download, often at a cost, and use.

Safety settings (profile): a set of customisable safety options linked to your online profile (see definition). Typically these options are related to opening of images and files, identifying trusted information providers and level of permissions for adult content.

Scan: the action or process of converting printed material to digital files by using a scanner. This conversion permits you to view them as electronic files on your computer and distribute them online.

Screen name: see definition for Nickname

Search engine: a tool used to search for information contained on websites. The most well-known are Google and MSN Search. Search engines have advanced user preferences that may include interesting safety settings.

Second Life: a well-known 3D web community provided by a US-based company, Linden Labs. Users can interact virtually via an avatar (see definition), create homes, various environments, trade and earn virtual currency, etc.

Sign-up: subscribing to an online service: newsletter, discussion forum, email, chat platform, etc. Normally, users should have the option to sign-out whenever they choose to.

SIP-Bench: a study supported by the European Commission that tested 30 control and anti-spam tools in order to measure their effectiveness in protecting children against harmful content on the internet.

Social networking: online communities of members who share interests and activities, and who interact and socialise online by the use of adequate software and services (see social networking sites).

Social networking sites: virtual platforms that host communities of members who share interests and activities. Members have to create user profiles and can share tools to upload texts, pictures or other files, post messages on message boards and take part in forums. Many social networking sites are prohibited to children under 13 year olds and provide safety profile settings.

Software: see definition for computer program

Spam: unwanted email, usually of a commercial nature, sent out in bulk. Spamming other people is definitely one of the most notorious violations of internet.

Spam filter: an application which blocks spam messages from being stored in your email inbox.

Spyware: malware secretly attached to files downloaded from the internet, which installs itself on the PC and monitors activity. It sends the information to a third party, often companies interested in defining personal profiles in order to send advertising or other information, or to crackers who want to gain access to private data.

Subscribe: to voluntarily register to a service or news update whereby information will be sent directly to your personal email inbox.

Toolbar: a set of icons or buttons that are part of a software program's interface. Toolbars serve as an always-available, easy-to-use interface for performing common functions.

Trial software: software which you can try before buying. Trial versions of software usually contain all the functionality of the regular version, but can only be used for a limited time.

Trojan horses: malicious code, malware that can enter your computer hidden behind harmless looking operations such as games or even virus-tracking programs. Trojans do not replicate themselves but are typically designed to access sensitive data or destroy data, and can erase a hard drive or steal confidential information.

URL (Uniform Resource Locator): the address of a specific web site or file on the internet. It does not contain special characters or spaces and uses forward slashes to denote different directories. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

User profile: a set of information describing a specific user of software, website or other technical tool. It typically includes information such as a username, password and other details (e.g. date of birth, interests).

Virtual possession: a set of objects that each player of a game is assigned with. Each player has virtual possession of his objects set via a computer terminal displaying the object set.

Virus: a type of malicious code, malware, designed to spread with user intervention. Usually it spreads through email attachments but also through infected external memory tools (USB stick, CD-Rom).

Voice over Internet Protocol (VoIP): a technology permitting users to talk over the internet, after downloading client software. The calls can be free of charge for users calling each other through the same VoIP client (e.g. Skype, Voicebuster). Such software also usually offers chat and file sharing facilities.

Wallpaper: a pattern or picture or other graphic representation that forms the background of your computer screen.

Web: short for World Wide Web. A collection of online documents formatted in HTML (HyperText Markup Language) that contain links to other documents as well as graphics, audio and video files. The web is a part of the internet.

Website: a location on the World Wide Web. Each website contains a homepage, which is the first document you see when entering the site. Sites usually contain links to additional files and sites. Websites are owned and managed by individuals, companies or organisations.

Webcam: a camera that can broadcast through the web, in instant messaging, PC video conferencing applications, chat platforms, etc. Web-accessible cameras include a digital camera which uploads images to a web server, either continuously or at regular intervals.

Worm: a special type of virus that is self-replicating and can spread without owner intervention across many computers and harm a network, consume tremendous bandwidth, shut a computer down, etc.

E. Useful addresses

WEBWISE.IE

The Internet Safety site in Ireland which provides advice and information for teachers, students and parents to help make online experiences positive and safe:
http://www.watchyourspace.ie

THE HOTLINE

To make a report about content that you have encountered on the internet which you suspect to be illegal, contact the hotline:
http://www.hotline.ie

WATCH YOUR SPACE

This website provides advice and information for teens on safe and responsible use of social networking websites like Bebo, MySpace, YouTube etc:
http://www.watchyourspace.ie

CHILDLINE ONLINE

Childline is 24-hour service for children and young people up to 18 years of age. It is open 365 days a year (even Christmas Day!) offering support to young people through the Childline listening service (1800 66 66 66) over the phone and through the website Childline Online. You can contact Childline for a chat or to talk about any problems you might have including internet related ones:
http://www.childline.ie

MAKEITSECURE

makeITsecure is a national awareness and information site focusing on the issue of IT security, specifically; phishing, spyware and identity theft:
http://www.makeitsecure.ie

SPUNOUT.IE

SpunOut.ie is a youth-led media initiative covering all aspects of youth info, health, lifestyle and activism. SpunOut.ie aims to guide young people through life with quality information, support and inspiration as well as providing a platform for young people to express their opinions, realise that they are not alone and get heard:
http://www.spunout.ie

INSAFE

The European e-safety awareness-raising network aims at empowering users to benefit from the positive aspects of internet use whilst avoiding the potential risks:
http://www.saferinternet.org

Supported by:

webwise.ie

ins@fe

chorus ntl:
a UPC company

Title: Family e-safety kit • Created by Insafe/Liberty Global-UPC in 2008
Prefix: 9789078209 • Id 51950 • ISBN-NUMBER: 9789078209577 • EAN : 9789078209577