//:WEBWISE: INFORMATION AND ADVICE FOR SCHOOLS://

tional Centre for Technology in Education
iúnta don Teicneolaíocht san Oideachas

//:WEBWISE: INFORMATION AND ADVICE FOR SCHOOLS://

webwise.ie

TABLE OF CONTENTS

INTRODUCTION

It is widely believed that the Internet has many pedagogical benefits. For example, the World Wide Web has the capacity to present information in a number of formats such as audio, video and hypertext, all of which are highly motivating for the learner. In addition, email, mailing lists and communication services have the potential to promote cross-cultural exchanges, language learning opportunities or other collaborative projects. However, there are also risks associated with Internet-based learning.

This publication is aimed at teachers who are involved in introducing safe online learning environments to their students. By outlining Internet safety issues in the context of education, it is hoped to empower teachers so they can make informed decisions about how to maximise the learning and teaching opportunities the Internet offers. Through presenting Internet safety teaching resources, this publication also provides a practical means for teachers to educate young people and help them develop the skills necessary for using all aspects of the Internet in a safe and responsible manner.

In addition, by exploring some of the risks associated with Internet-based learning, this publication seeks to present the argument that with appropriate precautions and a balance of measures, (including technical, administrative, evaluative and educational) safe and responsible use of the Internet can be achieved. The composition of these measures hinges on the educational needs and culture of each individual school. In light of this, different types of schools may tailor their approach to safe and responsible use of the Internet.

The NCTE recognises this fact and presents ***Webwise: Information and Advice for Schools*** as an adaptive resource that will enable individual schools to be proactive in the area of Internet safety. It is envisaged that this publication – and in particular, the sample Acceptable Use Policy – will be used as a basis for whole school policy development in the area of ICT integration.

National Centre for Technology in Education

The NCTE is a fully-funded agency of the Department of Education and Science. It was established in 1998. The centre has a wide remit in the area of ICT (information & communications technology) and education, extending beyond the use of ICT in schools to cover all educational ICT issues. Its main tasks are managing the implementation of the Government's ICT in Schools Programme, the development of ICT policy proposals and providing policy advice to the Department of Education and Science.

Webwise

Webwise is an Internet safety awareness initiative, developed by the National Centre for Technology in Education (NCTE) and comprising a range of online and printed information and advice publications for teachers, parents and students. It seeks to address key issues and findings arising from research conducted by the NCTE in Ireland over the past number of years relating to concerns about safety in regard to student use of and access to the Internet. The objectives of this initiative are:

- To promote the safe use of the Internet among school children (ages 4-18), their parents & teachers.
- To transform actual dangers into risks that they can master as autonomous, responsible users.

Other Internet Safety initiatives

The Government established the **IAB** (Internet Advisory Board), which includes membership from the service provider industry, Government, education sectors, the Gardaí, child protection interests and the legal profession. The IAB has the role of supervising the on-going evolution of self-regulation of Internet-linked organisations. The NCTE, as a member, works closely with this Board on all issues relating to safe use of the Internet.

The Hotline – http://www.hotline.ie – is managed by the Internet Services Providers Association of Ireland (ISPAI). It provides a central point of contact for members of the public who wish to report instances of potentially illegal content encountered on the web, for example, child pornography.

The European Commission's Information Society has established the **Insafe** network under the Safer Internet Programme. Insafe - www.saferinternet.org- is a network of national nodes that coordinate Internet safety awareness in Europe. The NCTE is the Irish member of the network.

NCTE'S RESPONSE TO INTERNET SAFETY

The NCTE's Internet safety strategy for schools includes a combined approach of the following actions:

1. Creating an acceptable usage policy (AUP).

2. Installing filtering or monitoring software.

3. Making students, teachers, and parents aware of the Internet risks and educating them to minimise these risks.

The NCTE, through its Webwise Internet safety initiative (www.webwise.ie) and through the ICT Advisory Service based in regional Education Centres, is providing support and advice to schools on Internet safety issues. Webwise focuses on raising awareness of online safety issues and good practice among students, their teachers and parents.

The Webwise website features a range of information, advice and tools including Internet Acceptable Use Policy templates, streamed videos, interactive online resources, advice sheets, and classroom activities. Webwise is the Irish node of EU Information Society's Safer Internet Network.

In addition to this, school Internet users should be aware that all schools connected to the Schools Broadband Network have a content filtering system in place which blocks illegal and harmful sites, pornography, hate sites and racist sites. Content filtering is provided centrally as a service of the Schools Broadband Network. This, however, does not preclude schools from having their own filtering system where a school wants to further refine online access within the school.

The NCTE is supported by a national network of 21 ICT advisors based in full-time education centres around the country. The ICT Advisory Service provides advice and support to schools on the safe use of the Internet in education through school visits and support nights. Webwise works with the ICT Advisory service to disseminate and distribute internet safety awareness information and tools.

The Teacher Skills Initiative (TSI) is a valuable multiplier in the dissemination of the "Safer Internet" message in Ireland. Currently some 14 courses for the continuous professional development of teachers have been developed by the NCTE in partnership with teaching professionals, third level institutions and teaching unions. The programme of courses ranges from a purely skills based focus to a pedagogical focus emphasising the practical application of ICT to teaching and learning. TSI working with Webwise have incorporated Internet safety components into the relevant internet focused courses for secondary and primary school teachers.

WEBWISE.IE

Minister for Education & Science, Mary Hanafin, T.D. launched the webwise website ***(www.webwise.ie)*** in February 2006. This website, developed by the NCTE, provides information and resources to teachers, parents and students to help ensure that children's on-line experiences are positive and safe. The website presents a technology-neutral message in four specific content areas: **surfing, chatting, sharing, and gaming**. All the resources to support the use of this education programme are available on **www.webwise.ie/surfwise**.

The webwise homepage contains up-to-date internet safety news, advice and information, and resources for teachers and parents. It helps you to find information about internet technologies; it tells you how they work, how young people are using them, and gives advice on how to minimise these risks of inappropriate use.

As well as providing information and advice the website also provides tools. You can access an online video for parents and teachers introducing the key internet safety issues and recorded presentations by members of the webwise team. There are sections that provide resources for schools such as legal advice on internet issues and templates for the formation of Internet Acceptable Use Policies in schools. There is also a learning resource section that provides access to lesson plans and activity sheets that can be used in the classroom.

NCTE RESEARCH

In order to understand how children are using the Internet it is necessary to investigate children's online activities. To this end the NCTE participated in a several studies that sought to gain knowledge on children's online risk behaviors and information needs. The findings of these surveys have been the foundation for all the internet safety resources developed by the NCTE. In 2003 the NCTE participated in a comparative analysis of children's use of the Internet with their counterparts in Norway, Iceland, Denmark and Sweden.

In January 2006 the NCTE carried out a large-scale survey of children's use of the Internet in order to identify their online risk behaviour. 848 students between the ages of 9 and 16 in over 21 schools across the country completed questionnaires containing over 100 questions on their use of the Internet. The findings from this survey will inform the development of Internet safety information, advice and tools by the Webwise Internet Safety in the coming years.

Research General Findings

In line with a general convergence and ubiquity in digital technology, the survey found that "all" children use PCs, 96% have used the Internet, and they have increasing access to the Internet through different devices such as personal computers, laptops, mobile phones, and game consoles. Almost 40% claim to own their own PC. 21% said they had internet access through a personal device such as a mobile phone or games console. This has implications for supervision and monitoring of children's use of Internet technologies. The survey found that over 50% of home PCs are not located in family rooms but in bedrooms or private rooms.

A quarter of the children surveyed said they used the internet at home everyday. One in ten use instant messaging (MSN, ICQ, Google Chat, Skype etc.) at home everyday or almost everyday. More than half are using the Internet at school more than once a week.

Many children are finding new friends on the Internet and other sources of support which are positive. One in fifteen of the children surveyed had met in real life someone that they first met on the Internet. This marks an increase from one in twenty-two in 2003. The majority of children said that they had a really good time during these meetings. In fact, in all cases where children met other children they reported positive or neutral experiences.

However, 11% of the 9 to 16-year-olds surveyed who met up with someone that they first met online said that the other person tried to physically hurt them. Worryingly, in all the cases of physical and verbal abuse reported in the survey the children said that the person who introduced themselves to them on the Internet as a child, turned out to be an adult. It seems clear that there are individuals who will use online services to make contact with children in order to exploit them.

Other General Findings:

- Half of the teenagers questioned said they had chatted on the Internet. Only a quarter of the preteens have ever chatted.
- 27% said they met someone new on the Internet who asked for information like their photo, phone number, street address, or the school they attend. This is an increase from 19% in 2003.
- A quarter of those who chat online use instant messaging everyday or almost everyday.
- 19% of those who chat said they had been harassed, upset, bothered, threatened or embarrassed by someone when chatting on-line.
- 23% have received unwanted sexual comments on the Internet. Boys are twice as likely as girls to receive them a lot.
- One-in-ten of those using the Internet use instant messaging everyday or almost everyday.

Research reports are available in the Publications section of the www.webwise.ie

Internet and Education Findings

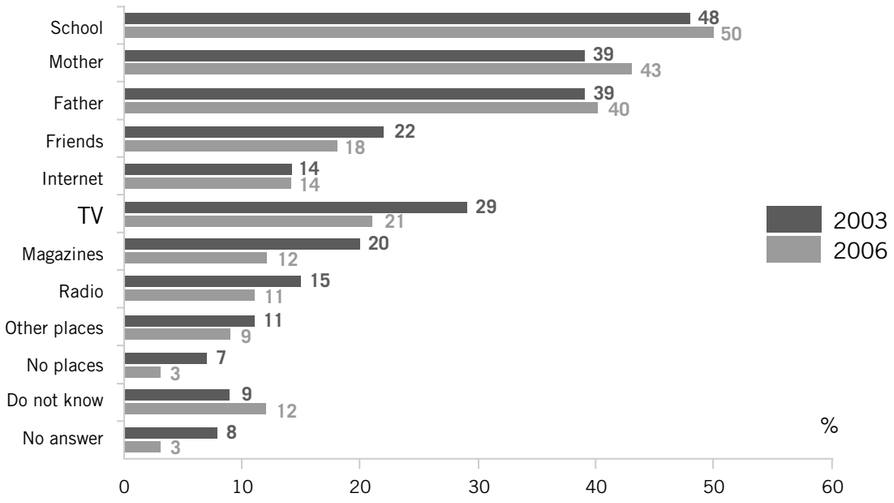
71% of children have had some form of instruction at school regarding use of the Internet. This shows an increase of 4% in the past three years.

17% said they received regular instruction. However when we asked what was covered by the instruction the most popular focus of instruction was on how to connect to the internet (54%). We know, that Internet use patterns change as children get older; we would hope that all children would receive regular instruction in this area so that the children would learn the critical competencies adjusted to fit their age group.

The education has mainly focus on the technical aspects of Internet use. Only 29% of those who received instruction got direction on how to protect their personal information. Pre-teens were more likely to get instruction in all aspects of how to use the Internet except for how to connect to the Internet.

The school, mothers and fathers are the main sources for Internet safety advice, and this is also from where they would like to get information in the future.

From what source would you like to get your Internet safety information?



Interestingly, teenagers would prefer to get their Internet safety information from school (49%), rather than parents (30%) or friends (20%). It can be assumed that this is because they are reluctant to alert their parents to the downside of the Internet for fear of having access withdrawn.

Other Educational Findings:

- 52% children use the internet at school more than once a week.
- 42% of the children said they use the Internet for doing homework.
- 24% of those using the Internet use it almost every day at home. 52% are using it at least once a week at school.
- 42% believe most or all of the information that they find online.
- 59% do nothing to confirm that information they find on the Internet can be trusted.
- 52% reported that their school work improved through using the Internet.
- In addition to asking their teacher or parent (67%), the Internet (42%) is now one of their main sources of information when doing homework

Research reports are available in the Publications section of the www.webwise.ie

INTERNET SAFETY IN CONTEXT

THE RATIONALE FOR INTERNET SAFETY

The Internet is rapidly becoming an increasingly popular research and communication tool at home and in school. Due to the fact that it is an unregulated medium, and has the capacity to host any type of information from online communities all over the world, the need for information and resources on Internet safety and related issues has never been more essential. Just like in the real world, the Internet has access to people and certain kinds of information that are unsuitable for children – and may potentially have a negative impact on children's attitudes, behaviour and well-being.

Although it is widely believed that the potential benefits of using the Internet as a learning tool far outweigh any risks involved, it is however important to be aware of the risks and their impact from the outset in order to equip students with the necessary information and skills to navigate safely on the Internet.

Education plays a central role in communicating risks and effective risk-reduction strategies to children, young people, and parents. Effective educational approaches should integrate parents as active facilitators of their children's media literacy and ability to self-manage potential risks in online environments.

RISKS ASSOCIATED WITH USING THE INTERNET

The Internet is central in the lives of young people today. It has been a truly transformational tool and has fundamentally changed the fabric of our society. We can also wholeheartedly say that the Internet can play a very positive role in the education and social development of our children. But it does have a downside. Inappropriate use and abuse of the same technology gives rise to a range of issues such as illegal content, harmful content, cyberbullying, and exploitation of children by commercial interests or predators.

Traditionally, we have considered the downside of the Internet in terms of children being "consumers" of online content. Some of this content could be pornographic, hateful or in some way damaging to human dignity. As adults, it is our responsibility to protect our children from this harmful content. However, this approach doesn't address the nature, scope, scale or extent of the risk of harm that may be associated with young people's current use of the Internet and new interactive Internet services. It doesn't consider the range of activities and behaviours which may pose a risk of harm to children and young people in online environments. In fact, they themselves may be the initiators of, and participants in, harmful online activities such as cyberbullying.

Young people interact in dynamic and very personal ways with their close friends and family and with chosen "online friends". The growth of blogs such as Bebo and MySpace — personal websites where people write up a diary or journal and rant about various topics — show that people are enthusiastic about actively sharing personal information and opinion. Children, having a heightened need to communicate and to be included in social networks, willingly exploit these online facilities and push the boundaries of use to create virtual "social networks". Many children see these online areas as private and free from adult and parental control and welcome the opportunity for regular and instant communication with peers. Adults need to be aware that very occasionally a child's virtual social activity can evolve into a real face-to-face meeting.

Exposure to illegal material

While the concept of illegal content is very much associated with child pornography, the terms cover a very wide range of issues. Illegal uses may be described under a number of headings including economic security, racial discrimination, pornography, privacy protection, gambling, and sale of controlled drugs, libel, and information security.

The Internet Services Providers Association of Ireland's (ISPAI's) publication entitled *Code of Practice and Ethics* defines illegal content as follows:

> *"Illegal" means content, which is contrary to criminal law.*

In 1998 the Irish Government Review Committee published Illegal and Harmful Uses of the Internet. This publication examines the negative issues associated with the Internet in the following way:

> *"While the concept of illegal use is very much associated with child pornography, the terms cover a wide range of issues. Illegal uses may be described under a number of headings".*

Below are the headings of illegal material, as categorised by this publication.

National Security
- Terrorist activities
- Instructions on bomb making
- Hacking into government computer networks

Injury to children:
- Child pornography
- Adult pornography
- Material depicting extreme violence
- Child trafficking
- Advice on anonymous exchange of graphic material

Injury to human dignity
- Racial discrimination, incitement to racial hatred
- Extreme sexual perversions

Economic Security
- All types of fraud
- Instructions on credit card piracy

Information security
- Malicious hacking

Privacy protection
- Unauthorised mailing
- Interception of personal email
- Misuse of personal data
- Unfair obtaining of personal data

Protection of reputation
- Libel

Gambling

Information on or sale of "controlled drugs"

Intellectual property
- Copyright infringements of any medium
- Unauthorised distribution of videos, music, software etc.

Source – Illegal and Harmful Use of the Internet
First Report of the Working Group, Government of Ireland, 1998.

Exposure to harmful material

Material on the Internet that is harmful can take the form of images, text, video and/or audio and may have a negative impact on children. The level of impact may vary, depending on factors such as age, emotional maturity and context of exposure. Nonetheless, exposure to harmful or illegal content may, in some cases, result in significant levels of fear, anxiety, imitation, disinhibition and desensitisation. Ideally, educators will seek to identify and discuss both the risks and the impact of such material at some level while implementing an Acceptable Use Policy (AUP).

More specifically, harmful material is difficult to quantify, as it requires an evaluation of its impact on different individuals. Material relating to sex, violence, terrorism, discrimination, crime, gambling, cult worship may be potentially harmful to some children but not to others. Discerning what may be considered harmful in a school setting is, therefore, an important aspect when devising and implementing an Acceptable Use Policy.

Whether or not access to this type of material is accidental, deliberate or unsolicited children may be faced with the temptation of viewing such material. Undoubtedly, students who deliberately search for sexually explicit material on the Internet will find the means of obtaining it – whether or not they have the technical skills to do so. Understanding the impact of such material is crucial to the quality of guidance and support teachers and parents can offer when educating students to protect themselves online.

The European Commission refers to using the Internet as a medium to communicate information which, while not illegal, might still have the capacity to affect the physical or mental development of vulnerable individuals, particularly minors. Harmful uses are difficult to identify with any great certainty as they involve an assessment of their effect on different individuals. This could include material relating to sex, violence, discrimination, graphic crime reporting, drug addiction, and cult worship. While not explicitly prohibited by law, this kind of material could, in the context of certain individuals, result in harm.

Harmful material has been identified as:

> *Content which includes any unlawful, libellous, abusive, offensive, vulgar or obscene material or any activities deliberately calculated to cause unreasonable offence to others, which whilst not necessarily illegal, is none-the-less considered inappropriate and deliberately calculated to cause unreasonable anxiety, inconvenience or stress to others.*
>
> ***ISPAI Code of Practice and Ethics, 2002***

There is a general acceptance amongst parents and educators that exposure to harmful material can often give rise to false and distorted beliefs about the world. Hateful content, such as racist content, is often believed if it is accompanied by plausible arguments or satisfies individual emotional needs. The intellectual limitations, emotional liability, immaturity and inexperience of children and young people make them particularly vulnerable to all this. Engrossment in any medium will affect a person's attitudes. Children and teenagers can be particularly impressionable as they are still in the process of developing their values. Intense use of undesirable material can create negative mind sets or exaggerate already established personality traits. Pessimism, personal antagonism, cynicism, unpleasant precocity, disaffection, diffidence, sexism, racism, intolerance and antisocial posturing are some of the possible outcomes.

Emerging Risks

Increasingly interactive Internet technologies and services increase the potential for children and young people to be exposed to a variety of risks which may result in harm to their physical and psychological well-being. The risk categories arise from the information sharing and dissemination capabilities of emerging technologies and services. These services provide opportunities for children and young people to communicate personal textual and visual information in publicly accessible and searchable online spaces.

These risks include the ability for children and young people to:
- Access illegal or age inappropriate content
- Experience inappropriate contact and communication with adults
- However, the key features and uses of many emerging technologies and services are changing the dynamics of risk, as they also provide opportunities for children and young people to become involved in the:
- Production and distribution of illegal and age-inappropriate content
- Initiation of inappropriate and abusive contact with others i.e., cyber bullying and defamation
- Experience of inappropriate and abusive contact from other children and young people

An additional category of risk is associated with the opportunities for online predators to use the capabilities of emerging technologies to:
- More easily access children and young people's personal information in order to identify potential victims
- Initiate contact and communication with children and young people
- Create false identities for use in victim identification and grooming processes
- Syndicate children and young people's content to other users of ill intent and widen their potential victim pool (Bryce 2006)

MINIMISING THE RISKS

Risks associated with the Internet can be minimised or prevented through education, awareness and by creating an infrastructure that facilitates the safe and acceptable use of the Internet for all members of the school community. Risk-reduction strategies need to be, flexible, responsive and predictive. Risk management should involve all key partners in developing a clear understanding of the risks and responsibilities associated with young people's use of Internet technologies and services.

This role of parents is vital in the promotion of safe online behaviour by children. They can play a key role as gatekeeper and guide to children's exploration of the Internet assisting them to critically evaluate and contextualise the information, opinions, and images they encounter. We should use educational strategies that integrate parents into the processes of enabling children to become increasingly autonomous responsible users of the Internet.

Since 2003 there has been a dramatic increase in the number of young people using the Internet at school. Apart from asking a teacher or family member, the Internet is now one of the main ways children seek information when doing homework. This increased integration of the Internet into young people's education brings the role of schools in the promotion of safe and responsible usage to the fore. Research shows that not only is the school one of the main sources of information about Internet safety but also it is their preferred sources, this is especially true for older children who named schools as the place that they wanted to receive guidance on safe use of the Internet.

REPORTING ILLEGAL CONTENT

If you have a serious concern that content / misuse encountered on the Internet may be illegal, you should report it to Hotline.ie. The www.hotline.ie service was established in November 1999 to combat illegal child pornography on the Internet.

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**.

Teachers who come across inappropriate material on the Internet through the Schools Broadband Network can contact the service desk to get it blocked. If you are aware of a website which may need to be blocked or re-categorised, contact the **NCTE Broadband Service Desk at 1800 334466**.

RESPONDING TO THE ISSUES

Devising an Acceptable Use Policy (AUP) is an important first step in addressing the issue of Internet safety at school level. The following information provides guidelines and advice on the issues involved in this process.

DEVELOPING AN ACCEPTABLE USE POLICY (AUP)

An Acceptable Use Policy is a document which addresses all rights, privileges, responsibilities and sanctions associated with the Internet. It is usually drawn up by teachers and management in consultation with parents, signed by students and their parents or guardians and often incorporated into the school's overall ICT policy. Ideally, every school will devise an AUP before it is involved in any use of the Internet and will seek Board of Management endorsement (for legal reasons).

AUPs may differ from school to school depending on school circumstances, student and teacher educational needs and technical infrastructures. It may be similar in the way it refers to sanctions or legal responsibilities.

Included in this publication is a sample AUP for teachers. In general, it addresses the safe, acceptable and responsible use of many aspects of the Internet. It also deals with sanctions to be imposed if the AUP is not adhered to. It may be used as a framework or customised to reflect individual school circumstances and needs. (This publication also includes guidelines on the use of different aspects of the Internet. These can be adapted or subsumed into the AUP provided, should the school opt to include that level of detail).

As the rationale for having an AUP is primarily to promote good practice and safe, responsible use of the Internet, it is a very important document. Its main goals are:

- To educate students, parents and teachers about the potential of the Internet as a valuable learning resource
- To define the parameters of behaviour and specify the consequences of violating those parameters
- To identify the school strategy on promoting the safe use of the Internet and address the risks associated with its use
- To provide schools with legal protection from liability

Explaining to students why an AUP exists and how it operates may sound obvious, but it is still an important step in raising awareness and providing students with insights into various Internet safety issues.

COMPONENTS OF AN AUP

An AUP should address all aspects of Internet usage. These include:

- Searching
- Downloading
- Publishing a school website
- Browsing websites on the World Wide Web
- Electronic communication such as email, chat rooms, newsgroups and other electronic forums

Other issues that an AUP may include:

- Electronic information research skills
- Where to locate Internet safety advice and guidelines
- Definition of inappropriate material
- Illegal and harmful use of the Internet
- Use of equipment for commercial gain
- Use of web-based email accounts
- Sanctions
- Copyright guidelines
- Online games
- Risks associated with use of the Internet
- Impact on student behaviour
- Reporting mechanisms
- Multimedia Messaging (This is a service provided by mobile phone companies that enables users to send and receive pictures and sound to or from other mobiles or email accounts.)

Suggested steps to follow in developing and updating this policy:

1	**Initiate and establish structures**	• Decide on who will have responsibility for putting this policy in place • Establish a co-ordinating group or committee, if considered necessary.
2	**Review and Research**	• Reference the key document *Webwise Information and Advice for Schools* which is a resource to support schools in being proactive in the area of Internet safety and is designed to be adaptable to the needs of individual schools.
3	**Preparation of draft policy**	• Print the following template materials below: ~ Sample Acceptable Use Policy (AUP) – template format ~ Permission slip for signature by parent/guardian – appended to template ~ Letter to parents/guardians ~ AUP checklist. • Amend the AUP to suit the needs of the school - each school's own context will influence the approach adopted.
4	**Circulation/ Consultation**	• Circulate the draft policy and consult with school staff, students, parents/guardians, board of management/trustees. • Amend the draft policy, as necessary, in light of the consultation process.
5	**Ratification and Communication**	• Present the policy to the Board of Management for ratification. • Make provision for the circulation of the policy to all parents/guardians and arrange to provide it to all students, including new entrants. • Communicate the ratified policy to other members of the school community.
6	**Implementation**	• Implement the provisions of the policy over a three week period initially.
7	**Monitoring**	• Check, at regular intervals, that the policy is being implemented and identify any issues arising.
8	**Review, Evaluation and Revision**	• Review and evaluate the impact of the policy (AUP checklist will assist this process). • Review it after the first three weeks of operation and at pre-determined intervals thereafter, and revise as necessary, in light of the evaluation process, feedback from school community and other developments.

INTERNET SAFETY: ACCEPTABLE USE POLICY TEMPLATE

School Name: _____

Address: _____

_____

The aim of this Acceptable Use Policy is to ensure that students will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school 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 school 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)

School's Strategy

The school 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 teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' Internet usage.
- Students and teachers 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 school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

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

Internet Chat

- Students will only have access to chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.
- 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.

School Website

- Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of students or staff.
- 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 student work will be co-ordinated by a teacher.
- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips of focusing on group activities. Content focusing on individual students will not be published on the school website with out the parental permission.. Video clips may be password protected.
- Personal student information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- The school will ensure that the image files are appropriately named– will not use students' names in image file names or ALT tags if published on the web.
- Students will continue to own the copyright on any work published.

Personal Devices

Students 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 unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

Links to the full text of these acts are available in the Resources for Schools section of www.webwise.ie

Support Structures

The school will inform students 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 written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

PERMISSION FORM TEMPLATE

Please review the attached school Internet Acceptable Use Policy,
sign and return this permission form to the Principal.

School Name _____

Name of Student: _____

Class/Year: _____

Student

I agree to follow the school'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 school.

Student's Signature: _____ **Date:** _____

Parent/Guardian

As the parent or legal guardian of the above student, 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 school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

I accept the above paragraph ❑ **I do not accept the above paragraph** ❑

(Please tick as appropriate)

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

I accept the above paragraph ❑ **I do not accept the above paragraph** ❑

(Please tick as appropriate)

Signature: _____ **Date:** _____

Address: _____ **Telephone:** _____

_____

_____

SAMPLE LETTER TO PARENTS/GUARDIANS

Dear Parent/Guardian,

Re: Internet Permission Form

As part of the school's education programme we offer pupils supervised access to the Internet. This allows students access to a large array of online educational resources that we believe can greatly enhance students' learning experience.

However, access to and use of the Internet requires responsibility on the part of the user and the school. These responsibilities are outlined in the school's Acceptable Use Policy (enclosed). It is important that this enclosed document is read carefully, signed by a parent or guardian and returned to the school.

Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access inappropriate or objectionable material.

The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the school's Acceptable Use Policy.

Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

Yours sincerely

AUP CHECKLIST

For an AUP to be robust it needs to be reviewed and updated regularly, taking into consideration implementation issues that may arise. The following is a checklist that may be used when developing or revising an AUP.

- ☐ Have AUP implementation issues arisen since the AUP was designed/revised?
- ☐ Have these issues been discussed with parents, students and teachers and incorporated into an updated AUP?
- ☐ Given that an AUP is in place, can the school confidently address the following scenarios?
  - ❑ A student is found using a chat room to arrange a face-to-face meeting with a friend.
  - ❑ The school uses filtering software but a student accidentally accesses a pornographic website while in your care?
  - ❑ A student publishes defamatory information on a personal website about a peer.
- ☐ Has the AUP had a positive impact on curriculum delivery?
- ☐ Has internal or external expertise assisted the formulation or reformulation of the AUP?
- ☐ Has the AUP as a code of Internet use transferred to home use?
- ☐ Does an open dialogue exist between students and teachers relating to Internet misuse and safety issues?
- ☐ Are teachers' and students' Internet safety training needs being met?

TECHNICAL OPTIONS FOR INTERNET SAFETY

Below is a description of the various technical options which can be used for safety in Internet-based learning. Once educators become aware of these options and their relative advantages and disadvantages, they will be able to make a more informed choice about the method most appropriate to their particular school context.

FILTERING SOFTWARE

Central to the debate on protecting children from inappropriate material on the Internet is the effectiveness of filtering software. Although filtering software reduces the risk of accessing inappropriate material to some degree, it should only be considered as part of a wider strategy to promote online safety. Relying primarily on filtering software may place students in a position of greater vulnerability if the filtering software fails to function effectively. Many teachers believe that fostering a culture of responsible use of the Internet is preferable and is in itself a valuable educational experience.

What is filtering?

Filtering is a term used to describe a way of limiting the content of web pages, emails, chat rooms and other electronic forums to which users may be exposed. Filtering software usually carries out the task of filtering. In general, filtering software operates using a set of criteria against which it judges whether Internet content is acceptable or not. For instance, the criteria could be a list of forbidden words, which the software seeks to identify on a web page or chat room. If the forbidden words are detected the filtering software blocks access to that location.

Filters operate by using one or a combination of the following:

- **White lists** or **allow lists**: Here, the software company compiles a list of websites that are perceived as appropriate for children of all ages and allows access only to these websites.
- **Black lists** or **deny lists**: This filter provides access to all sites on the Internet other than those contained in the black list. Due to the unregulated and changing nature of websites on the Internet, this type of system requires constant updating to be effective.
- **Keyword matches**: Here, the filter blocks sites which contain predetermined words or phrases that are considered inappropriate. It also removes offending words from a web page before being displayed.

Advantages

- Filtering software enables the administrator to have some technical control over students' access to the Internet.
- The fact that the software company compiles a list of inappropriate sites may be considered an advantage. With some software the user is allowed add to that list.
- Some software offers features such as time settings and user-group profiles. This allows filtering to be customised for different groups at different times.

Disadvantages

- In some cases, filtering software may be relied upon as the only Internet safety measure. This can result in a false sense of security in that while the filter will block websites on the basis of a URL (Uniform Resource Locator) or content, it cannot be guaranteed to block all harmful or illegal websites.
- The categories that filtering software companies use to assess material are predetermined and may conflict with the ethos and values of a school. For example, websites containing medical information or content relating to biological reproduction may be blacklisted.
- Over-blocking is possible with keyword matching, as the filter may not be able to make a distinction between different contexts. Again, this may result in blocking medical information or educational content relating to biological reproduction.
- Under-blocking may also occur as a result of the changing nature of content in web pages.

Schools Broadband network – Content Filtering

The objective of the Schools Broadband Programme is to enhance ICT in schools through the provision of a faster and secure network and online services. In this context, content filtering is used to enhance the schools ICT network environment so that it will better support the integration of teaching and learning. Content Filtering is an integral part of the Schools Broadband Programme, and involves allowing access to online content that is categorised as appropriate for schools while blocking access to certain web pages/websites or types of content that are categorised as inappropriate for schools.

The Schools Network security service facilitates the provision of an enhanced network environment for schools by carrying out the following functions on content being delivered through the schools network

- Allowing online access to websites or content that have been classified as appropriate for schools.
- Blocking viruses from external internet or email sources being sent to schools, note viruses can originate from websites or be received via email.
- Blocking other known 'malware' such as trojans, worms from websites or via email.
- Blocking SPAM (unsolicited email)

It should be noted that given the dynamic nature of the wider internet environment along with limitations of technology and human endeavour that no guarantees can be provided in terms of being able to protect schools from all inappropriate or harmful content. However the system in place is a 'best in class' solution, comparable or better than other systems deployed in educational situations worldwide. Online access from schools to Internet will be filtered using a Content Filtering system. The Filtering service provides Internet filtering which is based on 'Fortinet' services. Fortinet maintains and updates a database of over 27 million web sites. Any filtering service, no matter how extensive, can never be fully comprehensive, and schools are required to implement an Acceptable Use Policy (AUP) for all users in the school, and that adequate supervision of online access is maintained.

FIREWALLS

Firewalls are hardware or software systems that prevent unauthorised access to or from a private network. They are also the point of control that facilitates connection between different locations of the network. In general, they operate by checking and logging all passing electronic traffic and blocking data that does not match predefined security criteria.

Advantages

- A firewall has the ability to block Internet facilities such as websites, emails, newsgroups and chat rooms.

Disadvantages

- It will not block against viruses attached to emails although it may be able to monitor incoming virus codes transmitted from another part of the network.

WALLED GARDENS

Walled gardens refer to an online environment which usually consists of a collection websites that have been selected by a third party. Access to these websites is offered as part of a service by a company or ISP (Internet Service Provider) on a subscription basis. Walled Gardens are still relatively new and underdeveloped from an Irish perspective.

Advantages

- Walled gardens may provide a safe online environment for students.
- Educational sites and curricular resources can be pre-selected and made available.

Disadvantages

- Because the process of pre-selection and approval is granted by the ISP as opposed to the teacher, sites that are pre-selected may not be "age appropriate", address learning disabilities or relate to specific areas of the curricula.
- Walled gardens may not provide email, chat, search engine or newsgroup control mechanisms.

NETWORK SECURITY AND CONTROL SYSTEMS

Network security and control systems are hardware and or software packages that provide security, administration, monitoring and control functionality from a centralised location. Some systems may also provide additional features such as discussion forums and chat rooms. Altiris Vision and Ninaa are examples of such systems.

Advantages

- Records website addresses and screen shots of websites accessed by individual users.
- Provides access to users on a password basis.
- Allows users' computer activity to be intercepted or controlled at any time. This may be especially useful in a situation where students are using the Internet in different locations.

Disadvantages

- Some systems require additional hardware.
- Blocking inappropriate content may not be a feature of some systems.

MONITORING TOOLS

Monitoring tools generally refer to commercial or other tools that track a user's online activity with or without the knowledge of the user. At a basic level monitoring users' online activity can be done by checking the following files:

- History files
- Temporary Internet Files
- Cache files
- Cookies

Commercial monitoring systems can perform more advanced functions such as:

- Providing access to the Internet on an individual login basis.
- Displaying the content of the users monitor in real time.
- Recording keystrokes.

Advantages

- May work if combined with teacher supervision and education about responsible behaviour on the Internet.
- Provides a warning when an inappropriate image or inappropriate text is about to appear.

Disadvantages

- Not a blocking system and therefore relies entirely on the student's decision to view or reject illegal or inappropriate Internet content.

RATING SYSTEMS

Rating systems generally operate using "labels" to identify inappropriate material according to specific categories; for example, nudity, language, chat, violence etc.

Rating is normally carried out by a first or third party filling out a comprehensive self-rating questionnaire which focuses on what and how website content is depicted. Content providers and website authors are considered first party whereas third party refers to companies such as filtering companies. Most rating systems work in conjunction with web browsers or filtering software by reading the labels of sites and blocking or providing access accordingly.

These rating systems work under a set of protocols or standards known as PICS (Platform for Internet Content Selection).

Two popular rating systems are:

ICRA (Internet Content Rating Association), which is an international, self-governing group that rates and labels Internet content using broad categories such as sexual content, language, violence, nudity, gambling, alcohol and drugs. Internet Explorer, for example, uses ICRA ratings to block inappropriate sites.

SafeSurf, which uses a system to rate websites based on age level and content. It operates in conjunction with Internet Explorer and Netscape.

Advantages

- The responsibility of content regulation shifts from the government to web authors and organisations.
- Less expensive than filtering software.
- Authors of websites that have been developed for children can benefit from labelling their site, as some search engines construct their database of "safe sites" by using labels.
- Labelling pornographic or "adult only" sites places a responsibility on the operator to self-regulate. This can appeal to many operators, who may prefer the prospect of credit card owners – as opposed to young children – visiting their sites.

Disadvantages

- Websites may be rated inaccurately or be biased.
- Websites that don't carry ratings may be blocked for that reason.

GUIDELINES FOR SAFE USE OF THE INTERNET

BROWSING THE WORLD WIDE WEB

The World Wide Web (www) can be considered a virtual library of information; as a result, many schools use it to find information published by other schools, governments, universities, companies and teacher organisations.

One of the most compelling aspects of the World Wide Web is the ability to locate information by clicking on words or images – otherwise known as HTML (Hypertext Mark-up Language). This allows the user to navigate or browse web pages in a linear or non-linear fashion as they wish. In order to browse in this way an application known as a browser is required. The most popular browsers used are Internet Explorer and Firefox.

Benefits

- Exposure to a wide variety of educational material in multi-media formats.
- The ability to broaden information research skills.

Risks

- Exposure to illegal or harmful material.
- As the WWW is made up of web pages of information where any member of the global community can be an author, the validity of information available may often be questionable or inauthentic. Students need to be taught the necessary skills to be able to discern the validity of content on web pages.

Guidelines

Setting up content

- Preview or evaluate websites and internal links before providing student access. Alternatively, use an education web portal such as Scoilnet (**www.scoilnet.ie**) as a means of sourcing websites that have been previewed and approved by educators.
- Ensure online learning is directed and task-oriented. Consider the use of WebQuests (see below) or curriculum-focused websites such as TeachNet Ireland.
- Bookmark websites and encourage student to locate websites in this way.
- Consider offline browsing (see below) or the implementation of a virtual learning environment such as Blackboard for controlled access to the Internet.

Administration

- Ensure pupils do not have the master Internet password of their Internet service account.
- Place computer in an area of the class where the monitor is clearly visible.
- Have the ICT co-ordinator regularly monitor all Internet usage.
- Set time limits for Internet use to discourage aimless surfing.
- Keep a record of which students are allocated to each pc and how long they have been online. This can be done automatically or by employing specialised applications.

Student awareness

- Encourage any student who accidentally encounters illegal material to switch off their monitor immediately and report it to their teacher.
- Teach students how to evaluate the content validity of websites. A sample model entitled Webwise Checklist has been provided as part of this publication.
- Ask students to ignore or close marketing banners that appear on certain websites.
- Remind students of any aspect of the school AUP and sanctions that relate to browsing the Internet.

Offline browsing

As mentioned above, offline browsing can be an alternative to browsing the Internet using a live connection. The main advantage of this is that it reduces the inconvenience of heavy traffic, broken network connections and sites that no longer exist. A download manager or Internet agent such as WebWhacker can facilitate the process of downloading an entire website, including text, graphics and HTML links directly to a hard drive.

It is important to note that current copyright law is, generally, in favour of limiting the use of downloaded materials to classroom and student use. It is, however, advisable to check if copyright law relates specifically to downloading entire websites from the Internet.

WebQuests

A WebQuest is a discovery-based activity that presents student groups with one or more problem-solving tasks on a given topic. It usually takes the form of a website which is published by students or teachers and which contains links to online resources on various aspects of that topic.

Students begin the WebQuest by learning some common background knowledge, then dividing into groups and taking on individual roles and tasks. The idea is that individuals effectively become experts on one aspect of the topic. Finally, students combine their learning by completing a summarising activity, for example, presenting their analysis to real world experts.

Virtual learning environments

Virtual learning environments (VLEs) are web-based interfaces that assist learning and teaching by providing and integrating online resources and tools. Although mainly used for distance education and at third level, virtual learning environments are increasingly being explored and tested by schools at primary and post primary level. There are many commercial products on the market, including Blackboard, TopClass, LearningSpace and WebCT. However, there is no reason to presume that independent tools could not be combined to create an online learning environment.

In general, virtual learning environments contain the following features:

- A facility for the delivery of materials.
- A file upload area for teachers and students.
- A tool for timetabling, posting to notice boards and using a calendar.
- A communication mechanism, i.e., one to one, one to many, synchronous and asynchronous (chat rooms, email, newsgroups etc).
- Password based access.
- Conferencing tools.
- Multimedia resources.
- An administration tool for student tracking and compiling progress records.
- Class lists and student homepages.
- A self-testing tool.

For related links and further information on browsing the World Wide Web visit **www.webwise.ie**

WEBWISE CHECKLIST

The Internet hosts a wide range of websites – personal, commercial, educational and so on. However, the credibility of some websites or organisations may be questionable, therefore presenting a risk to children's online safety. The following **Webwise Checklist** may be used as a starting point for teachers or students to assess the credibility and safety of various websites.

Website title: _____

URL: _____

This website contains the following features:

- ❑ A Privacy Statement is automatically provided.
- ❑ The site is updated on a regular basis.
- ❑ The website title is indicative of its content.
- ❑ Icons, images and text that link externally to other websites can be easily identified.
- ❑ The copyright status of the information contained on the website is such that information can be reproduced for educational purposes.
- ❑ The author has indicated the source of their materials where necessary to do so.

This website contains a chat room with the following safety features:

- ❑ An ignore button. (Allows you to ignore a particular chat user).
- ❑ Facilitated/supervised chat sessions.
- ❑ A reporting facility. (This is useful if material is, or users are, offensive).
- ❑ A facility to save chat conversations.

Other safety considerations include:

- ❑ The name of the author is clearly stated.
  TIP – The author's name is usually near the top or the bottom of the page. If you can't find a name, check for a copyright credit (©) or link to an organisation.

- ❑ The name of the organisation can be clearly identified.
  TIP – Check the domain name of the organisation (eg .com, .org, .edu, .gov, .net) as the type of organisation behind a website can give an indication of its credibility.

- ❑ There is information about the author's credentials.
  TIP – Look for biographical information or the author's affiliations (university department, organization, corporate title, etc.)

- ❑ There is a contact phone number, email address and postal address for the author and/or organisation.
  TIP – Check for a "Contact Us" or "About Us" section.

SEARCHING THE WORLD WIDE WEB

The Internet offers a wide variety of exciting resources that can be incorporated into many school-related activities. Many teachers recognise this fact and often create lesson plans or activities that involve students searching independently for information.

Using a **search engine** is one way of locating web pages or any other material on the World Wide Web. A search engine is a type of program that retrieves a list of web pages relating to a keyword search. Some examples are Alta Vista, Google, Lycos and Excite.

Subject directories are also useful tools for finding material on the WWW. A subject directory is a catalogue of sites that has been composed and structured by people – rather than generated by a computer program. Usually it presents information by category and subcategory.

The following information provides an overview of the benefits and risks associated with searching the WWW, and also suggests some guidelines.

Benefits

- It allows students to engage in discovery-based learning at a pace that suits individual learning needs.
- It provides students with an opportunity to develop research skills and critically evaluate material on the World Wide Web.
- It enables students to build and share information which is motivating and educational.
- Interesting websites and resources may be bookmarked or stored in the "favourites" folder for future reference.

Risks

- Access to illegal or harmful material.
- Wasting time on skimming through pages of results or irrelevant material.
- Encountering advertising banners.

Guidelines

Below is a list of guidelines that may be useful in ensuring that (a) independent searching of the Internet during a lesson is effective and (b) the risk of accessing irrelevant or inappropriate material is minimised for students.

- Consider using search engines that have been designed for students with Internet safety in mind. These include:
  - http://www.askforkids.com/
  - http://yahooligans.yahoo.com/
  - http://www.education-world.com/
  - http://sunsite.berkeley.edu/KidsClick!/
- Agree with students on what is considered as targeted or relevant information and what is seen as distractions to the task at hand.
- Some children in Special Education may need to be directed to use certain key words, and have proper spelling of them provided.
- Be clear about your search topic and related concepts. For example, you may wish to search for "children's websites."
- Develop a list of search terms, for example, synonyms or alternative spellings for each concept, for example, "kids sites".
- To search for derivatives of a word, consider using a "wild card" or "truncation" symbol such as an asterisk (*) at the end of a word. This will retrieve all words that begin with that root.
- Refine the search by putting three words inside quotation marks, for example, "Internet lesson plan". This will return only pages, which have all three words next to each other.
- To connect terms, most computer systems use logical connectors (known as Boolean operators) such as **AND**, **OR** and **NOT**.

  AND ensures that ALL search terms are present.

  OR ensures that ANY one search term is present.

  NOT excludes unwanted terms.

Google Safe Search

Google's SafeSearch screens for sites that contain explicit sexual content and deletes them from your search results. No filter is 100% accurate, but SafeSearch should eliminate most inappropriate material.

You can choose from among three SafeSearch settings:

- **Moderate** filtering excludes most explicit images from Google Image Search results but doesn't filter ordinary web search results. This is your default SafeSearch setting; you'll receive moderate filtering unless you change it.
- **Strict** filtering applies SafeSearch filtering to all your search results (i.e., both image search and ordinary web search).
- **No** Filtering, as you've probably figured out, turns off SafeSearch filtering completely.

You can also adjust your SafeSearch settings on the Advanced Search or the Advanced Image Search pages on a per search basis. These pages can be accessed by clicking the Advanced Search link beside the search field in Google.

Other Considerations

Some teachers may also prefer to:

- Preview and select suitable websites before students begin their own searches.
- Test results of child-friendly search engines for the age appropriateness of content.
- Use education indexes or portals such as **www.scoilnet.ie** to locate specific education material.

Finally, if students are to benefit from searching the Internet independently, they will require instruction, guidance and assistance. This will allow them to develop and refine their searching and evaluation techniques, learning skills which may be considered valuable and lifelong.

DOWNLOADING

The Internet is a virtual library of multimedia resources, some of which can be downloaded and used to motivate the learner or enrich learning experiences. Pupils with various learning styles can also benefit from downloading material such as pictures, text, audio, video or software programs which they can then incorporate into projects, presentations or publish on the World Wide Web.

Downloading generally means when the user copies a file from an online service to their own computer. This file may be a web page, graphic, game or program and can either be free or commercial.

The following information provides an overview of the benefits, risks and guidelines associated with downloading.

Benefits

- Downloading programs or material for offline use may reduce charges associated with connection to the Internet.
- Downloading provides access to freeware (software which is free) or shareware (software which is accessible for a trial period and has limited functionality compared to the full version.)

Risks

- Spread of viruses: A virus is a piece of code that is deliberately designed by someone with the intention of causing damage to files on a computer. It operates by attaching itself to some other program or downloaded file.
- Covert gathering of user information: Spyware or Adware refer to programs that may be hidden in some freeware or software. This type of software gathers user information through their Internet connection without the user's knowledge or consent, primarily for advertising purposes.
- High Internet connection fees due to poor bandwidth or the abuse of bandwidth resulting from downloaded spyware.

Guidelines

- Install and update anti-virus and anti-spyware software. This, in conjunction with good housekeeping, can greatly reduce the threat caused by computer viruses.
- All floppy disks should remain within the confines of the computer room. It is not advisable to let students bring them home and then return them to the school.
- When the sender of an email is unknown to the recipient, avoid clicking on attachments containing an executable file.
- Check if spyware is present by consulting a database of spyware products such as http://www.spychecker.com.
- Websites may be downloaded for offline use using programs such as WebWhacker, WebFerret etc.
- It is considered good practice to seek permission from a website author or designer before reproducing material for educational use.

Other Considerations

- Ensure that pupils understand the rules and regulations for using and reproducing material that is copyrighted.
- Inform students of the benefits and risks of freeware, shareware, clipart and public information.

EMAIL

Electronic mail or email is a communication tool that allows people around the world to send text (and non-text items) to each other. Communication by email is probably the most frequently used application and the most compelling aspect of using the Internet. Email sent via the Internet normally arrives at its destination in a matter of seconds.

Broadly speaking, there are two scenarios for accessing email in schools with the most common being the first described below. Here, students can send or receive emails internal to the school using a class, school or personal email account; in this case, sending both internal and external emails is usually conducted under the supervision of a teacher.

The second type of email access in schools is the use of web-based email such as "hotmail" or "yahoo". This may be considered unrestricted personal email access as it means that teachers are unable to monitor the content of student emails. It is important to note that NCTE does not endorse the use of web-based personal email access for students in schools.

Benefits

- Allows students to communicate and share ideas and resources with teachers and students all over the world.
- Students can engage in collaborative projects with online peers.
- Can help improve students' writing and communication skills.

Risks

- Receipt of spam (electronic junk mail), which may be offensive, controversial or of an illegal or harmful nature.
- Contact with unsuitable social groups or people who disguise their identity.
- Receipt and distribution of viruses and chain mail.

Guidelines

- Consider using class-based email addresses such as rangultan@scoil.ie whereby students have a degree of anonymity.
- Educate students to resist forwarding chain mail as it clogs the network and increases the downloading time of legitimate emails.
- Advise students not to open email attachments when the sender is unknown to them as such attachments may contain a virus.
- Ensure that students are aware of reporting procedures in relation to receiving illegal or harmful material.
- Never click on "remove email from mailing list" as this validates your email address and ensures future spamming.
- Consider implementing filtering software that offers a facility to filter email. (A web-based tool such as http://www.mail2web.com will allow you to check all emails on your server before downloading. This enables you to manually delete spam or inappropriate material.)

COMMUNICATING ONLINE

Revolutionary developments in ICT allow us to be active users of communications media. Using web tools like Instant Messenger and Bebo young people are interacting in dynamic and very personal ways with their close friends and family and with chosen "online friends". The growth of blogs - personal websites where people can write up a diary or journal, rant about any topic and, more importantly, a place where your friends can find you - show that people are enthusiastic about actively sharing personal information and opinion.

Teenagers, having a heightened need to communicate and to be included in social networks, willingly exploit these online facilities and push the boundaries of use to create virtual social networks. Many teenagers see these online areas as private and free from adult and parental control but allowing opportunities for regular and instant communication with peers.

Benefits

- It is the cheapest way to stay in touch with friends
- May enhance language-learning opportunities and collaborative projects.
- Presents opportunities to interact with mentors or subject specialists.
- Allows people with similar interests to share information and collaborate with each other despite geographical separation.
- Facilitates the inclusion of schools otherwise marginalized because of geographical location and enables e-twinning – nationally, with in the EU and worldwide.

Risks

- The Internet allows users to be anonymous. It is impossible to really know who you are communicating with, so deception becomes easier. This means that online contact has the potential to result in harmful or exploitative contact in real life.
- Increased access to communications technology has led to the heightened possibility for cyber bullying
- Contact with people who disguise their true identity.
- Disclosure of personal details such as a/s/l (age, sex, location).
- Invitation to a face-to-face meeting.
- Exposure to harmful or illegal material.

Guidelines

Listed below are guidelines designed to help teachers use online communication services as effectively and safely as possible.

Physical environment

- Allocate a computer or group of computers for communication use, where 'chat' can be easily monitored.
- Position the computer so that the monitor faces outward.
- Always ensure that the usage is supervised by a teacher who is familiar with the technology.
- Set time limits and prepare material relevant to the subject for discussion.

Choice of Service

- Use educational interactive services that are age and/or ability appropriate.
- Ensure that there is a facility that allows conversations to be saved.
- Ensure that there is a facility to report offensive users.
- Consider the use of usernames.

Student awareness

- Nominate a student in each class/group to chat as part of an organised activity and report information gathered to the class.
- Inform students of the risks associated with interactive services.
- Remind students of how the school AUP addresses use of these technolgies.
- Stress that any online bullying or receipt of illegal material should be reported immediately to the teacher supervising the session.

- Educate students to stay in the public areas. Children are often invited to "whisper" which means to leave the public area and engage in one to one communication.
- Advise students against disclosing personal information.
- Advise students to practise good netiquette, i.e. etiquette on the Internet.

Other considerations

The school needs to consider how to address the likelihood of a student revealing their true identity or personal details on the Internet, either by accident or deliberately. It is advised that this type of scenario be covered in the school AUP. Some schools may operate a policy whereby they alert parents to any instance relating to disclosure of identity.

Finally, teachers shouldn't be afraid to utilise interactive services in a controlled way in their teaching as this can create many educational possibilities. However, unmonitored, unstructured access is not advised.

Stranger Danger

The most serious risk of using the internet involves the possibility of a child being lured into a physical encounter with someone they've met online. Sadly, cases have been reported where predators have used the Internet to initiate contact with a child, gain their confidence and ultimately to arrange a face-to-face meeting.

The Internet has played an important role in the grooming process for sexual predators trying to make contact with children. A typical scenario for a sexual predator might be as follows:

- Following the initial contact in a public area of a social networking website, the predator could invite the child into a private area to get to know them better.
- Next in the grooming sequence comes private chat via an instant messaging service, and then e-mail, phone conversations (often on mobile phones).
- The final step in the process is a face-to-face meeting.

The grooming process can go on for weeks and months, as it may take this long for the child to feel truly comfortable. The patience of the predator may also be explained partly by the fact that it is not uncommon for them to be grooming several children at the same time.

Cyberbullying

"Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others." –Bill Belsey, (www.cyberbullying.org)

Cyberbullying includes the following:

- Sending offensive, cruel or threatening messages, emails, photos or film
- Silent phone calls.
- Posting malicious comments or pictures on a bulletin board, website or chat room.
- Pretending to be someone else in a chat room or message board or text message and making malicious comments
- Accessing someone's accounts in order to scare them or cause trouble for them.

Cyberbullying is different from other forms of bullying in the following ways:

- 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 malicious or cruel messages on the back of a school book and posting them on the Internet is that 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 don't fear being punished for their actions.
- This type of behaviour is often outside of the reach of schools as it often happens outside of school on home computers 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 don't always know their cyberbullies.
- Communications technology has become ubiquitous. As a result, Cyberbullying can happen any time and any place and for many children, home is no longer a safe haven from bullying.

PUBLISHING A SCHOOL WEBSITE

Publishing a school or class website presents a wide range of learning opportunities for both teachers and students. Often, as students with advanced technology skills become project leaders, teachers take on a new role as either facilitator or learner. Through this activity, curricular resources can be shared, collaborative projects can be undertaken and the school can be promoted within the wider community.

Benefits

- Students and teachers are given an opportunity to learn technical skills related to web authoring.
- Students gain an appreciation of the online publishing process (planning, creating storyboards, content development, teamwork, testing, evaluation, editing etc.) and publishing for a wider target audience.
- Students gain an insight into roles and responsibilities associated with project work.

Risks

- Photographs of children may be downloaded by social groups for illegal use.
- The publication of personal details may place students at risk of being contacted either face-to-face or online by other users.

Guidelines

- Identify the purpose and structure of the website.
- Define what is considered appropriate for publication on the school website. This should be included in the school AUP.
- Consider who has access to the server aside from the IT Co-ordinator. Assign roles and responsibilities to those classes or teachers who manage information on the web server.
- Never publish class lists.
- Photographs of children should focus on the activity they are engaged in.
- Never publish a student's name beside their photograph.
- Permission to publish student work, photographs, video or audio clips should be sought from parents either as part of the AUP or independently.
- Reference student work by username.
- Consider copyright laws, privacy rights and data protection regulations.

Other considerations

- Consider the need for editorial responsibility.

In the context of the Internet, identifying editorial responsibility and accountability can be very difficult. There is no legal requirement that material published on the Internet have an identified editor. However, if it is possible to identify the editor of online content then that person, or persons, may be held liable for their involvement. In respect of large websites, different parts of a site may have different editors and this will most likely be the case with schools.

- To avoid online plagiarism, seek permission to use copyrighted content from the website author. A permission template available from **http://www.landmark-project.com/permission1.php** can be used for this task.

NEWSGROUPS/DISCUSSION FORUMS

Newsgroups, discussion forums and message boards are electronic forums where ideas and knowledge can be exchanged. The term "Usenet" refers to a collection of newsgroups.

Currently there are thousands of newsgroups covering a range of different topics. Unlike chat rooms, newsgroups, discussion forums and message boards do not function in live or "real" time.

Benefits

- Teachers and students can talk to experts, share ideas and experiences.

Risks

- Exposure to illegal or harmful material.
- Flaming: flaming refers to a barrage of angry messages directed towards a person or persons. It is considered to be bad manners to flame someone.
- Contact with unsuitable social groups.
- Most forums are not edited for content and anyone with an Internet connection can easily send in contributions.

Guidelines

- Check if a licensing agreement or additional newsreader software such as "Free Agent" is necessary.
- Consider which forums are provided by the school's ISP (Internet Service Provider).
- Are there any forums in general that are relevant to the needs of the school and the delivery of the curriculum?
- Be informed about how the school intends to monitor the use of newsgroups of each class.
- Stress to students the importance of reporting inappropriate material and online harassment to teachers and relevant organisations.
- Consider downloading a free discussion board forum from the Internet and incorporating it into the school website or intranet.

Blogs

Blogs (short for "web logs") are basically online diaries or journals. They are relatively easy to set up, and are quite cheap, or often free, to maintain. They are popular among teenagers, but are also used by journalists, authors, politicians and other professionals to keep in touch with their readers, supporters or clients. They can be password protected or open to all Internet users (just like regular websites). Some also have the facility for readers to post messages and make comments.

Benefits

- Enables students to gain an insight into the day to day activities of various professions.
- Enables students to create and share online journals for projects.

Risks

- Students may be tempted to divulge personal information online.
- Possibility of exposure to online bullying.
- Possibility of accessing blogs with illegal or harmful content.
- Possibility of contact with unsuitable social groups.

Guidelines

- Are there any blogs that are relevant to the needs of the school and the delivery of the curriculum?
- Be informed about how the school intends to monitor the use of blogs in class.
- Stress to students the importance of reporting inappropriate material and online harassment to teachers and relevant organisations.
- Use of individual students' names online should be avoided.

NETIQUETTE

The term "netiquette" is a compound of the words "network" and "etiquette". It refers to maintaining good manners when interacting with others while online. The following are basic guidelines for netiquette with regard to email, chat rooms, discussion boards and newsgroups. Teachers may find these useful when fostering standards of Internet behaviour among students.

Email netiquette

- Use proper spelling, grammar and capital letters, even if this isn't always the standard in email.
- Seek permission of the original sender before forwarding their email or it may be perceived as an invasion of privacy.
- Use humour and sarcasm with care, as messages can easily be misinterpreted. Consider using 'smileys' (emoticons) if you need to indicate to the reader that you are joking. Keep in mind that overuse of emoticons can be viewed as annoying.

  :-D Laughing
  :-(Sad
  :-e Disappointed
  :-) Happy
  :-@ Screaming
  :-I Indifferent
  :-o Surprised
  :-< Mad
  ;-) Winking

- When replying to a message, copy and paste the content of that message and include your response to each part of the original message.
- Use acronyms (for example IMHO = in my humble opinion, BTW = by the way) sparingly, as readers may not know what they mean.
- Never send a message that you wouldn't want to be shown to others.
- It is considered impolite to use capitals in your subject line or in your message as it is viewed as the equivalent of SHOUTING! To make a point, try using *asterisks* or _underscores_ around the word or phrase you wish to stress.
- Prior to sending very large files, seek permission from the intended recipient. Some people may have slower connections and therefore this may impede the downloading process.
- Check with recipients before emailing "carbon copies" of jokes. Some people do not appreciate this use of email.

Chat room/discussion boards/newsgroup netiquette

- Visit a discussion board prior to allowing student access, as it will enable you to get an insight into the type of messages and responses that are posted.
- Keep messages relevant to the group.
- Use meaningful subject headers.
- Include a notation in your subject line, for example, [long message] if you are posting something that's particularly lengthy.

BASIC TECHNICAL STEPS

There are a number of basic technical steps for using Internet browser utilities that can minimise some risks associated with access to the Internet. These include adding favourite sites, using Content Advisor and checking history files, temporary Internet files, cache files and cookies. The following is a step-by-step guide to assist teachers in introducing these basic technical measures.

ADDING FAVOURITE SITES

- Open a site that you visit regularly in the browser.
- Select **Favourites Menu**.
- Click **Add to Favourites**.
- In the **Add Favourite** window, the web page address appears as the **Name** bar of the page.
- Click **OK** or alternatively type a more descriptive name and then click **OK**.
- Click on the **Favourites** menu tab and the contents of your **Favourites** folder appear as a drop down menu.
- The selected site has been added to the list.

USING CONTENT ADVISOR (INTERNET EXPLORER BROWSER CONTROLS)

Content Advisor is a tool that can be set to allow or deny access to specified websites.

- Click on **Control Panel** in the **Start Menu**.
- Double-click the **Internet Options** icon.
- Click the **Content** tab.
- In the **Content Advisor** section, click **Enable**.
- Click on the options *Language, Nudity, Sex, Violence* and adjust the slider accordingly. The rating slider is not visible until you select one of the categories in the Category window. Click on **Language**. The slider has five stopping points that correspond to the five levels. Dragging the slider over and back changes the Level number and a short description.
- The **More Info**... button connects to the **ICRA** Web site
- Decide upon the levels for each **Category** then click **Apply**
- **Click** on the **Approved Sites** tab.
- Enter the addresses of sites that are either **approved** or **disapproved**.
- To approve a site, enter the address and click on the **Always** button.
- The approved site appears on the **List of approved and disapproved websites**: preceded by a small green icon.
- To block sites, enter the address and follow the same steps but click the **Never** button. Disapproved sites appear with a red circle on the list of sites.
- As **ICRA** is a voluntary system, the number of non-rated sites far outweighs the number rated. The **Content Advisor** blocks non-rated sites by default and will demand a password to view all such sites.
- Click **Apply**.
- You are now prompted for a **Supervisor Password**. This will be necessary for editing the settings of the **Content Advisor** in future.
- You will be asked to confirm your password when using the **Content Advisor** for the first time.
- Click **OK**

Once the **Content Advisor** has been **Enabled**, if a blocked site is accessed a dialogue box appears to inform you the site is blocked.

CHECKING HISTORY FILES (INTERNET EXPLORER)

History files allow you access to websites and pages visited in previous days and weeks. To access these files follow these steps:

- Double click on your browser (you may be using Internet Explorer, Netscape Navigator or Firefox).
- On the toolbar click on the **History** icon. On the left, the History bar appears, containing links to websites and pages visited in previous days and weeks.
- Click a "week" or "day" in the History bar: this gives you access to a website folder which displays individual pages. Click the relevant page icon to display the web page you wish to see.
  ~ The History bar can be hidden by clicking the History button again.

CHECKING TEMPORARY INTERNET FILES (INTERNET EXPLORER)

The Temporary Internet Files folder contains all the web pages that have been visited recently. Web pages are copied to this folder so that any websites visited previously can be loaded quickly. To access temporary Internet files, follow these steps:

- Choose **Internet Options** from the **Tools** menu in Internet Explorer
- Click **Settings** in the Temporary Internet Files part of the **General** tab.
- **Choose View Files**.

COOKIES

Cookies are messages that are sent to a web browser by a particular website. These messages are stored on your computer and are sent back to the website each time you visit it. The function of cookies is to record your activities on a particular website so that the next time you visit it you are presented with customised information. Cookies are recurrently used in "adult" and commercial websites and in most instances you are required to complete a form that requires disclosure of personal information.

On the other hand, since cookies are stored on your computer it is possible to view them in order to find out the addresses of websites that have been recently visited. To view cookies, follow the same steps as you did to access cache files (see above). Cookies may be identified by name, Internet address, type, size and so on.

LEGISLATION

There is no specific legislation governing Internet safety at school level. Complicating this issue is the fact that the Internet functions in a global context whereas the law operates in a localised one. There are, however, a number of legislations that have relevance to Internet safety. They are briefly described as follows:

- **European Communities (Electronics Communications Networks & Services) (Data Protection & Privacy) Regulations 2003 (S.I. No. 353 of 2003)** - These regulations, among other things, prohibit the sending of unsolicited direct marketing messages (e.g. SPAM) unless the recipient has given their prior consent.
- **Data Protection (Amendment) Act 2003** - This amendment extends the data protection rules to manually held records and also makes improvements to the public's right to access data.
- **Child Trafficking and Pornography Act 1998** - This act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.
- **Interception Act 1993** - (The Interception of Postal Packets and Telecommunications Messages Regulation Act 1993). This act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.
- **Video Recordings Act 1989** - This act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer. It would apply where someone in the State supplied this kind of video over the Internet.
- **Data Protection Act 1988** - This act was passed in order to deal with privacy issues arising from the increasing amount of information kept on computer about individuals.

COPYRIGHT AND FAIR USE GUIDELINES

Copyright

Great care must be taken in relation to the use of material from websites. Almost everything created privately and originally after April 1, 1989 is copyrighted and protected whether it has a notice or not. Publication on the Web does not mean it is not copyright protected. You should assume a work is copyrighted and may not be copied, unless you know otherwise.

Fair Use Guidelines for Students and Teachers

Between 1992-1994, a group of publishers and educators gathered to agree to more specific guidelines so educators would not be sued for copyright infringement when they were thinking their copying was "fair use." In determining "fair use" the factors to be considered included -

- the purpose and character of the use including whether such use is of a commercial nature or is for nonprofit educational purposes
- the nature of the copyrighted work

Students may:

- incorporate portions of lawfully acquired copyrighted works when producing their own educational multimedia projects for a specific course
- perform and display their own projects in the course for which they were created
- retain them in their own portfolios as examples of their academic work for later personal uses such as job and school interviews.

Educators may:

- incorporate portions of lawfully acquired copyrighted works when producing educational multimedia projects to support their teaching needs
- present their projects in the following situations: face-to-face instruction, assign projects to students for directed self-study, remote instruction (with limitations).
- retain their projects indefinitely for the following purposes: to perform or display in presentations to their peers, for example, at workshops and conferences, to retain in their personal portfolios for personal uses such as promotion or job interviews.

- use their projects for teaching, for a period of up to two years after the first instructional use with a class. Instructional use beyond that time period requires permission for each copyrighted portion incorporated in the production.

Limitations on Size/Portions for both Educators and Students

Motion Media

- Up to 10% or 3 minutes, whichever is less, of a single copyrighted motion media work.

Text Material – Poems

- An entire poem of less than 250 words, but no more than three poems by one poet, or five poems by different poets from any single anthology.
- In poems of greater length: up to 250 words but no more than three excerpts by a single poet, or five excerpts by different poets from a single anthology.

Music, Lyrics and Music Video

- Up to 10% but no more than 30 seconds of music and lyrics from a single musical work
- Any alterations to a musical work shall not change the basic melody or the fundamental character of the work
- A photograph or illustration may be used in its entirety.
- No more than 5 images by an artist or photographer.
- Not more than 10% or 15 images, whichever is less, from a single published collected work.

The Educators Guide to Copyright and Fair Use can be found at
http://www.techlearning.com/db_area/archives/TL/2002/10/copyright.html

Copying and Distribution Limitations

Including the original, only a limited number of copies may be made of a project:

- two use copies, one of which may be placed on reserve.
- an additional copy for preservation to be used or copied only to replace a use copy that has been lost, stolen, or damaged.
- for jointly created projects, each principal creator may retain one copy but only as permitted by use and time restraints previously outlined.

Attribution & Acknowledgement

Credit the sources and display the copyright notice © and copyright ownership information for all incorporated works including those prepared under fair use.

Copyright ownership information includes:

- © (the copyright notice)
- year of first publication
- name of the copyright holder

Notice of Use Restrictions

The opening screen of a program and any accompanying print material must include a notice that:

- Certain materials are included under the fair use exemption of the U.S. Copyright Law
- Materials are included in accordance with the multimedia fair use guidelines
- Materials are restricted from further use

Future Uses Beyond Fair Use

If there is a possibility that a project could result in broader dissemination [for instance, publication on the Internet], whether or not as a commercial product, individuals should take steps to obtain permissions during the development process rather than waiting until after completion of the project.

Rules Of Thumb For Coursepacks

- Multiple copies must conform to previous "fair use" rules (not to exceed, in any event, more than one copy per student in a course)
- One chart, graph, diagram, drawing, cartoon or picture per book or per periodical issue
- There shall not be more than nine instances of such multiple copying for one course during one class term.

Obtaining Permission

Contact: **http://www.utsystem.edu/OGC/IntellectualProperty/permissn.htm**

Remember that these are copyright guidelines and not copyright laws. When using material from a Web site, check the copyright link (often found at the bottom of the Home page) to check the specific Copyright laws relating to that site.

The larger corporate Web sites will have Web pages that expressly state that the content of the Web site is copyrighted and may not be copied or used in any way other than for the purpose it was created.

EDUCATION

The NCTE has produced Internet Safety education programmes and resources that are available in the Learning Resources section of the webwise website. These education programmes include an introduction to the topic for teachers, classroom and take-home activity sheets, and lesson plans. There are many other education resources available online, below are some of the resources that we recommend.

TEACHING RESOURCES ON INTERNET SAFETY – PRIMARY

SurfWise Education Programme

Description: Webwise has developed engaging interactive resources including an animated-lesson, video clips, interactive questions and related classroom activities. Students using these resources will discover some of the things they can do online, what to do if they come across something that makes them fell uncomfortable and that not everything on the internet is what it seems.

Preparation: In order to view animations, this site may require a Flash player which can be downloaded from the following website. http://www.macromedia.com/shockwave/download/alternates

As the site also uses audio headsets are required.

URL:

Interactive Resources: http://www.webwise.ie/Surfwise.aspx

Surfwise lesson: http://test.scoilnet.ie/webwise/lessons/index.html

Learning to surf activities: http://www.webwise.ie/GenPDF.aspx?id=787

Source criticism activities: http://www.webwise.ie/GenPDF.aspx?id=783

Completion time: 5 x 45 minutes depending on ability range of class.

Surf Swell Island (Disney)

URL: http://disney.go.com/surfswell/index.html

Preparation: In order to view animations, this site may require a Flash player which can be downloaded from the following website. http://www.macromedia.com/shockwave/download/alternates

As the site also uses audio headsets are required.

Description: The Disney website provides an interactive game in four parts which deals with a wide range of issues and challenges children to think about privacy, behaviour on the Internet, protecting against viruses and using emoticons. Children are invited to progress through each challenge in a linear fashion, picking up jewels until they eventually receive a certificate in the Treasure Palace section.

Completion time: 10–15 minutes depending on ability range of class.

Kidscom

URL: http://www.kidscom.com/games/isg/isg.html

Preparation: If playing for points, which enables students to enter competitions, preparation time will include seeking parental permission and registering. The site uses audio so therefore headsets are required.

Description: This site contains an Internet safety game, which includes a cloze test and a task that requires the user to unscramble sentences containing safety messages. It can be played without or without being a registered user. The site has many other interesting features, some of which require parental permission in order to participate.

Completion time:15 minutes depending on the group's literacy ability.

NetSmartz (National Centre for Missing & Exploited Children (NCMEC))

URL: http://www.netsmartz.org

Preparation: This site requires Flash player and each activity takes a few minutes to download. As the site also uses audio headsets are required.

Description: This site provides an interactive workshop on various aspects of Internet safety and is entitled NetsSmartz Kids. It deals with issues such as identity deception, protecting personal information and meeting people online. It also offers free screen savers and wallpaper containing Internet safety messages. In addition to the Internet safety workshop, the overview section on the NetSmatz Parent's and Educator's page provides a link to age appropriate classroom activities.

Completion time: Including downloading time approximately 5 minutes per activity.

TEACHING RESOURCES ON INTERNET SAFETY – POST-PRIMARY

Know IT All

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

Preparation: This site requires Flash player and each activity takes a few minutes to download. As the site also uses audio headsets are required.

Description: The purpose of KIA is to help students reflect on their own use of communication technology, be aware of the dangers and develop safe and discriminating behaviour when using new technology. The content addresses a number of issues relevant to the national curriculum in information and communication technology (ICT), personal, health and social education (PHSE), citizenship, and media literacy. You can download a full 2 page overview of KIA

Completion Time: Each section may take 10 minutes to read depending on literacy levels.

Various Lesson Plans

URL: http://www.cybersmartcurriculum.org/lesson_plans/

Preparation: Printing and previewing each activity may take a few minutes. In order to read the pdf files, Adobe Acrobat may need to be downloaded from the following website.
http://www.adobe.com/products/acrobat/readermain.html

Description: This is an excellent source of ideas and lesson plans covering five units relating to Internet safety, which are aimed at primary and junior level post-primary students. Lesson plans and resources are available in both online and offline formats and can be downloaded as pdf files.

Completion time: approximately 20 minutes per lesson.

KEY SUPPORTS

Webwise (http://www.webwise.ie)
Provides information and advice on Internet safety issues for teachers and parents.

Hotline (http://www.hotline.ie)
Irish hotline for reporting online child pornography. Reports can be made by emailing report@hotline.ie or phoning 1890-610710

Internet Service Providers Association of Ireland (http://www.ispai.ie)
An organisation that represents the Internet Service Providers industry at national, European and international level.

An Garda Síochána (http://www.garda.ie)

IAB (Internet Advisory Board) (http://www.iab.ie)
Established by the Minister for Justice, Equality and Law Reform in 2000, with a general remit to supervise a system of self-regulation by the Irish Internet Service provider industry.

Safer Internet Action Plan (http://www.saferinternet.org)
The Safer Internet Action Plan is the European Union's response to promoting safety on the Internet, addressing the controversial issue of illegal, harmful and racist content.

ISPCC – Childline Online (http://www.childline.ie/)
Sometimes children can just be looking for information but find it difficult to talk to someone. Childline provides these support pages as a place to start.

Barnardos (http://www.barnardos.ie)
Barnados is a leading independent agency for children and families.

COPINE (http://www.copine.ucc.ie)
The COPINE Project is an initiative which addresses the issue of child exploitation via the Internet.

GLOSSARY

Anti virus software
A software program that can be installed to scan and protect files from computer viruses.

APNIC (Asia Pacific Network Information Centre)
A non profit organisation that registers and administers IP addresses. APNIC databases can be searched to identify and trace emails.
ARIN (**A**merican **R**egistry for **I**nternet **N**umbers) and **RIPE** (**R**éseaux **IP E**uropéens Network Coordination Centre) are similar organisations.

AUP (Acceptable Use Policy)
An agreement specifying appropriate and inappropriate use of the Internet.

Bebo
Bebo 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, their favourite films and music and post up photos of their lives. Bebo links people together through the schools and colleges. This is significant in Ireland because Bebo has an extensive database of Irish schools and colleges that users can join.

Bookmarks
A collection of personal websites of interest to the user. Bookmarks operate in the same way as putting a marker in a book, making it quick and easy to navigate the World Wide Web. By bookmarking websites, it is possible to prevent children accidentally accessing inappropriate material through misspellings.

Browser
The software that allows users to read pages on the WWW World Wide Web.

Browser history
A folder, stored by the browser, which contains recently visited websites.

Cache
A special computer data storage area (memory or disk) where frequently used data values are duplicated for quick access.

Chat room
A place where you can have a conversation with one or more people in real time, that is, when you type in a line of conversation the other person sees it immediately and can reply straight away.

Cookie
A piece of information or message sent by a web server/website to a web browser in order to gather data on how a user uses a website. Depending on the type of cookie used, and the browser's settings, the browser may accept or reject the cookie. Cookies may contain information such as user preferences, registration or login details relevant to a particular website.

Domain name
A unique name that identifies an Internet site. Separated by dots, domain names have two or more parts, for example, ncte.ie.

Download
The process of transferring a copy of an electronic file from a remote computer to the requesting computer by means of a modem or network.

Email
Short for electronic mail. A text or non-text message sent from one person to another by means of a computer.

Filtering software
A program developed to sort and block access to undesirable material on the Internet. Normally operates using a list of banned sites and approved sites which has been compiled by the software company.

Firewalls
Hardware or software systems that prevent unauthorised access to or from a private network.

Flame
(verb) To pass a derogatory comment.

FTP
Short for File Transfer Protocol. A method of transferring files from one computer to another over a network.

HTTP
Short for HyperText Transfer Protocol. A protocol for transferring hypertext files to the Internet.

HyperText
A system in which objects (text, pictures, music, programs and so on) can be creatively linked to each other, permitting the user to browse through related topics regardless of the order in which the topics are presented. A hypertext link (hyperlink) is the point of access to additional information on a web page or CDROM.

ICQ ("I Seek You")
A commonly used instant messaging program that is downloaded onto a computer. It enables users to chat, email, perform file transfers and play games.

Internet
A network consisting of many millions of computers around the world, connected together by telephone lines, cables and satellites.

Internet Service Provider (ISP)
A company that provides Internet connection to its customers. ISPs normally provide e-mail accounts and website space as part of the service.

Instant Messaging (IM)
A communication tool that enables you to create a private chat room with another person. Typically, the instant messaging method notifies you whenever somebody on your private list is online. A chat session with that particular individual can then be initiated.

Internet Protocol (IP)
A unique identifier for a computer or other device on a TCP/IP network.

IRC (Internet Relay Chat)
A commonly used chat room program which allows real-time conversations.

MMS (Multimedia Messaging Service)
This service facilitates the sending and receiving of messages comprised of text, image, video and sound to and from mobile phone handsets or computers.

Newsgroups
An Internet facility that allows users with a common interest to exchange information. There are many thousands of newsgroups, often updated many times a day. They may be moderated or unmoderated.

Proxy server
Also known as cache server. Used by Internet Service Providers to hold cached web pages.

Social Networking
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, growing the total number of members and links in the network. The value of the network for members is exponentially linked to the number of people in the network. Social networking sites offer features such as automatic address book updates, viewable profiles, the ability to form new links through "introduction services," and other forms of online social connections. These networks tend to be organized around shared common interests. MySpace, for example, builds on independent music and party scenes, and Bebo is organised around schools and colleges.

Spam
Junk mail that shows up in email boxes or on newsgroups, generally advertising a product.

TCP/IP
Abbreviation for **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol. The suite of communications protocols used to connect computers on the Internet.

URL (Uniform Resource Locator)
An address that enables web users to locate information at different websites on the World Wide Web. Example: http://www.ncte.ie

Usenet
A worldwide system of newsgroups and discussion groups that uses the Internet and other networks.

Virtual Learning Environments (VLEs)
Web-based interfaces that assist learning and teaching through providing and integrating online resources and tools.

Web browser
A software application used to locate and display web pages. Examples include Netscape Navigator and Microsoft Internet Explorer.

World Wide Web
An information search, retrieval and publishing system for the Internet. This system contains a network of servers which support documents that are written in a format known as HTML (Hypertext Markup Language).

YouTube
YouTube is a popular free video sharing web site which lets users upload, view, and share video clips.