

Internet Safety



The Internet is becoming an increasingly popular research and communication tool at home and in school. As in the real world, the Internet may allow 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 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.

There are three categories of risk associated with children using the Internet.

- Exposure to illegal and/or harmful images and text, whether violent, racist or explicit in nature.
- Receipt of messages that are demeaning, threatening or in other ways disturbing or detrimental to a child's wellbeing.
- The possibility of being lured into a physical encounter that might threaten a child's safety and wellbeing.

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

1. Making students, teachers and parents aware of the Internet risks and educating them to minimise these risks.
2. Installing filtering or monitoring software.
3. Creating an acceptable usage policy (AUP).

Raising Awareness

The NCTE, through its Webwise Internet safety initiative (www.webwise.ie) and training courses 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.

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.

Content Filtering

Content Filtering is an integral part of the Schools Broadband Program and involves allowing access to online content that is categorised as appropriate for schools while blocking access to web pages/websites that are categorised as inappropriate for schools.

The centrally managed filter on the Schools Broadband network

- Allows online access to websites or content that have been classified as appropriate for schools.

- Blocks viruses from external internet or email sources being sent to schools. (Note viruses can originate from websites or be received via email).
- Blocks other known ‘malware’ such as Trojans and worms from websites or via email.

It should be noted that given the dynamic nature of the wider internet environment along with limitations of technology and human endeavour 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.

School Acceptable Use Policy

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). Acceptable use guidelines for schools are available on the Webwise.ie website.

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. 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.

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.

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, instant messaging, VOIP and other electronic forums

Adequate supervision of children’s use of the Internet in schools is vital. Controlling access to the sites and services visited by children and ensuring that they act responsibly while online are important steps in the process. Children should be informed that their online activities will

be monitored and that they are accountable for their behaviour. Other steps to be taken include:

- Close monitoring of children's activities during Internet sessions
- Advising students to use moderated chat rooms only
- Preventing e-mail attachments from unsolicited or unknown sources being opened
- Directing online activities to previously evaluated educational resources or previously sourced safe sites
- Installing appropriate blocking/filtering software — this software, while not entirely foolproof, will greatly reduce the risk of deliberate or inadvertent access to undesirable material
- Prohibiting registration or the signing of visitors' books at Web sites without permission

E-mail and Chat

The school's Acceptable Use Policy should contain guidelines for participation in Internet sessions, web-based chat, or e-mail correspondence. These guidelines should include the following information:

- No personal information about the child, the child's family, teachers or the school is to be disclosed without permission from the teacher supervising the session
- Any encounter with information or a message that threatens, demeans or otherwise makes the child feel uncomfortable must be reported to the teacher supervising the session and under no circumstances should a response be made to such a message
- On no account should a child make arrangements for an unsupervised meeting with any other online correspondent without permission
- If permission is obtained, any planned meeting should be supervised and should occur in a public place
- Pictures or images which might assist in identifying an individual should not be transmitted without permission
- Use of a full or last name in online correspondence should not occur without permission

School Web Sites

The following precautions should be taken when developing and maintaining content for the school Web site:

- Children's work should appear in an educational context with a notice prohibiting the copying of such work without the expressed written permission of the school
- No home address, telephone number, contact details or personal student information should appear with such work
- The inclusion of portrait style or small group photographs should be avoided – use large group photographs if necessary
- No name, home address, telephone number, contact details or personal information should appear with student photographs
- If a Web page is inviting contact from other Internet users, use a school or class e-mail address, not a personal one
- The school should obtain parental permission prior to publishing pupils' work or photographs of pupils

Data Protection Act

The Data Protection Act (1998) was passed to deal with privacy issues arising from the increasing amount of personal information kept on computers about individuals. In giving rights to individuals, the Act also puts responsibilities on schools holding personal information about pupils (both in terms of school administration and school Web sites). Given this fact, schools should:

- Only publish pupil information that is relevant to the content of the Web page being assembled – additional or superfluous information should not be published
- Inform parents about pupil information being published on the school's Web site

Relevant Web Sites

Webwise

www.webwise.ie

Webwise is the Irish Internet Safety Awareness Node managed by the NCTE. Webwise provides parents, teachers, and children with educational resources, advice and information about potential dangers on the Internet and empowers users to minimise or avoid these risks. Webwise shares best practice, information and resources with European partners through the European Commission's Insafe network.

Insafe

www.saferinternet.org/ww/en/pub/insafe/index.htm

Insafe is a network of national nodes that coordinate Internet safety awareness in Europe. The mission of the Insafe cooperation network is to empower citizens to use the Internet, as well as other information and communication technologies, safely and effectively. This site contains a monthly newsletter on Internet Safety and a repository of resources and key players in internet safety.

Internet Child Pornography Hotline

www.hotline.ie

To make a report about content that you have encountered on the Internet which you suspect to be illegal, contact the hotline via this link.

Internet Advisory Board

www.iab.ie

The Internet Advisory Board was set up to make sure that self-regulation worked in practice and to actively monitor developments in the complex and fast-changing area of internet service provision. The board comprises public and private sector bodies such as the ISP Association of Ireland, the Police Force, the NCTE, the Irish Hotline, Barnardos and the Department of Enterprise.

Note: While the advice sheets aim to act as a guide, the inclusion of any products and company names does not imply approval by the NCTE, nor does the exclusion imply the reverse. The NCTE does not accept responsibility for any opinions, advice or recommendations on external web sites linked to the NCTE site.

This Advice Sheet and other relevant information are available at:

www.ncte.ie/ICTAdviceSupport/AdviceSheets