

SAFEGUARDING

NEXT
GENERATION
LEARNING

April 2010

Further Education and Skills

Becta leading
next generation
learning



Safeguarding

in a digital world

Guidance for learners

Technology

in everyday life

Information and communications technology (ICT) is part of our lives. We use it every day for study, work, entertainment, shopping and getting in touch with our family and friends.

The world of work and business expects us to develop skills to use ICT confidently to promote improvements. It's one of the quickest and easiest ways of finding information, sharing ideas and working with other people.

And like everything else we've ever invented, from the bow and arrow onwards, it has to be used safely and responsibly. As well as the opportunities, there are also risks that we need to be aware of and guard against.



RELATED PUBLICATIONS

Using technology safely is vital to further education staff and learners alike. There are four publications in the **Safeguarding in a digital world** series.

1. Safeguarding in a digital world: An overview for learning providers

2. Safeguarding in a digital world: Guidance for curriculum managers, teachers and training staff

3. Safeguarding in a digital world: Guidance for technical staff

4. Safeguarding in a digital world: Guidance for learners

The risks

By using information and communications technology, and particularly the internet, you are potentially allowing other people to have access to the system you are using, giving them information you might not want them to have or even breaking the law.

The risks can be summed up within the four Cs:

Content – it's easy to download all kinds of material, but some of it may be illegal, dishonest or inappropriate. For example:

- music, films, for example are someone else's intellectual property and may be protected by law
- any material that you research and then present in your own work must be properly referenced and credited to whoever created it – passing it off as your own is plagiarism
- you may come across content that is offensive, such as pornography or incitement to hatred or extremism – it should be reported, not passed on
- social networking sites are great for sharing information about yourself to your friends but they are very public. For instance, employers are increasingly looking at them when they recruit, so think before you post.

Contact – sites like chat rooms allow you to meet new friends but not everyone is who they claim to be. Don't give out information that could make you vulnerable to exploitation, bullying or sexual aggression.

Conduct – Behaviour like bullying, racism, harassment and piracy is just as bad when displayed in the online world as in the real world. You have a right to be protected and a duty to behave honestly and responsibly. When you are using someone else's system, such as your training provider's, don't do anything that makes them vulnerable to malicious software or charges of bad behaviour or lawbreaking by downloading or passing on illegal or inappropriate content.

Commerce – internet shopping is convenient, but make sure you know how to protect yourself from online scams and identity theft. Check that a site belongs to the company it says it does – if in doubt look for a real world postal address or phone number. Be wary of sites selling unprescribed medical drugs or that promote online gambling.

Who is responsible for managing this risk?

E-safety is a partnership between you and your learning provider. It's a balance between allowing you access to information and sites you want to use, and that support you in your studies, and keeping you, other learners and the organisation safe.

Your provider will draw up an acceptable use policy (AUP). You will be expected to abide by it, but you should also be consulted about the rules.



FURTHER INFORMATION

Next steps

What should I do now?

These are typical questions which you need to consider when using information and communication technology when studying, socialising and working to enhance your e-safety:

- Are you aware of the acceptable use policy (AUP) in relation to the use of information communication technology issued by your learning provider?
- Have you been given an opportunity to develop and comment on the AUP?
- Do you bring your own technology into your training provider? If so, do you know how the AUP applies to your use of your digital kit on your learning provider's premises?
- Are you aware of the need to protect your personal information when you are online and how to do this?
- Do you know where to go to download music, videos and other media legally? Are you aware of the penalties in place if you download material illegally?
- Do you know about plagiarism and are you aware of the potential consequences?
- Do you always check the source of emails, instant messages and files you receive online before opening them in case they contain viruses?
- Do you know who you can go to if you receive information which contains unacceptable content or contains information you find offensive?

Get Safe Online:
awareness and advice
www.getsafeonline.org

BBC Webwise:
internet safety quizzes
www.bbc.co.uk/webwise/course/safety/menu.shtml

NetSmartz (USA):
lesson plans and resources
www.netsmartz.org/netteens.htm

Childnet International:
awareness and advice
www.childnet-int.org

Digizen – advice and resources:
www.digizen.org

Direct Gov's Click Clever Click Safe campaign
<http://clickcleverclicksafe.direct.gov.uk/index.html>

Think U Know:
awareness and advice
www.thinkuknow.co.uk

Report abuse, via the Child Exploitation and Online Protection Centre
www.ceop.police.uk/reportabuse

The UK Hotline for reporting illegal content
www.iwf.org.uk

Anti-Bullying Network
www.antibullying.net/cyberbullying5.htm