Safeguarding learners online:
A checklist for FE & skills learning providers supporting 14-19 learners working with technology

These guidelines are to help you prepare for and act upon the issues you will have to face when using technology with young learners who are coming to you as part of your partnership working with schools and/or as part of 14-19 Consortia. Now that technology is part of everyday life and the work environment, learners will need to be able to use it safely and securely wherever they are learning, as it is an essential part of their learning experience.

For FE & Skills providers who are new to teaching younger learners and the 14-16 age group in particular, this guidance will help you tackle any concerns you may have about protecting younger learners and maximising the benefits of using technology, without exposing your organisation to unnecessary risk. The guidance is for all FE & Skills providers, but in particular we hope that work-based learning providers and work experience providers will find this useful as a focus for this key strategy for safeguarding your business.

Relevant advice developed by Becta and other agencies has been signposted throughout this document. There is a Glossary of more technical terms appended that may be useful to you.

For this guidance we have taken a Risk Assessment approach. This is normal practice for activities that may lead to unsafe behaviour or legal difficulties. In the case of online activity your learners and staff should be clear that behaviour guidelines should apply equally to online and offline behaviour.
The first section gives an overview of the key issues that you need to know about; for further advice and guidance see the Becta and Excellence Gateway web sites.

Hazards relating to working online

These are often categorised as Content, Contact and Commercial risks.

Illegal or inappropriate content

Issues relating to *copyright* and *illegal download* arise regularly, especially if learners see your system as offering an opportunity to by-pass their home provider restrictions; this may lead you into legal difficulties. Downloading music and video from peer-to-peer networks is common practice amongst teenagers (however the BBC iPlayer also uses this technology).

You need to ensure that your staff have a good understanding of the legal requirements surrounding the recording and storage of images of their learners, especially if they are thinking of using their own equipment.

Visit the TASI website for useful guidance. (Further links below).

Learners will need constant reminders of the need not to *plagiarise* from the internet, especially during criterion based assessment when it may be more difficult for the learner to demonstrate the authenticity of their own work. The usual good practice of keeping records of work-in-progress, along with effective Functional ICT skill building will mitigate this. An emphasis upon Reflection, as defined in the Personal Learning and Thinking Skills element of the Diploma, will help to support the change in attitude required. Younger learners are often resistant to redrafting work, so it's essential to allow them to use technology to support them in this process, from simple tools like the spell-check, recording images to reflect upon their progress in a practical task, or making an audio commentary upon their work.
The JISC Plagiarism advice service is free to most FE & Skills providers – though not to all WBL providers, so do check with your local RSC - and can help you to identify plagiarised material; it is listed in the links section below.

Pornography, or material that incites racial hatred or violent extremism are types of materials that may be accessed by some young people as they engage in experimental and perhaps risky behaviour as part of the process of growing up.

The use of *social software* or *video sharing sites* like Facebook, MySpace, YouTube and others should be considered as part of the learning experience – employers are increasingly putting resources onto them – but bandwidth issues as well as behaviour may affect your decision to allow access. Learners can become distracted if they have open access to social software sites, and their high use of bandwidth, affecting the speed of connection of the whole network, is commonly quoted by practitioners as the main reason they block them. Some FE providers allow the teaching staff but not the learners to access these sites; or restrict access within normal teaching hours. Others have had success in controlling access by carefully tailoring the amount of download space each learner is allocated after a dialogue with staff who run their course – some courses require more than others but having a conservative limit can focus the learner effectively on using the correct procedures. Learning platforms can give instant feedback and monitor the use of storage space for the learner and the provider and the potential to use podcasting, video and audio clips in a safe and secure environment.

Learners within the 14-19 age group need to understand the implications of using social networks like MySpace on their long term prospects; many employers routinely search online for records of potential employees. Since these tools are now becoming very widely used, there may be cases where members of staff are

in danger of putting themselves or your organisation in disrepute; staff should have a clear understanding of your position on using them. There are many resources useful for educating learners and staff about the use of social networks; see the links list for examples.

Contact

Inappropriate contact with adults has been a high profile aspect of internet safety reports, though such incidents are relatively rare in education. Since the Children Act (2004), anyone up to age 18 is a 'child'. You have the same responsibilities to younger learners when they are working online as you do when they are being taught face to face, so you should be able to control who they are in contact with online, as well as offline, while they are with you. Don't forget that online contact can be very effective in building up a relationship, so that everyone they are in contact with as part of their learning should have had appropriate checks and training (see for example the LSIS Safeguarding module in the link list below).

It's worth highlighting the particular vulnerability of learners with special needs and disabilities. They may well be more trusting, take things more literally, be less cautious and more open in responses. This means that those supporting them may need to be more vigilant. Educating these youngsters about working safely online may need to be more measured and over longer periods. See the Curriculum staff checklist below.

Bullying

Learning providers should make it clear that bullying someone using a digital device like a mobile phone, or via on-line communication like MSN – often called cyber-bullying - is no different than during face-to-face encounters. There is no difference in harassment produced by using online messages from that using verbal abuse. In extreme cases, often reported as 'happy slapping', physical bullying has been recorded and sent around using mobile phones or social networking sites, but bullying via text messages, or compromising images, can be just as distressing. There are concerns too about victimisation of staff by learners using technology. This could be exacerbated if staff lack confidence using new technologies and again clarity of policies and clear penalties for any breaches of codes of conduct is necessary to reassure staff and protect the organisation.
The use of 'malware' computer viruses to harass or bully an individual is not often reported but should be covered by an adequate anti-virus policy (see advice to Technical staff below)

Grooming

The processes of accessing illegal content and inappropriate contact, even of 'grooming' vulnerable young learners by predatory or fanatical adults are well publicized in the media. Some FE and Skills learning providers have had incidents that have had to be dealt with sensitively, yet thoroughly. You need to be confident that you have minimised any risk to your organisation while they are with you. Most importantly you should ensure that you can produce adequate records, when required by the authorities. Internet Service Providers should adhere to the internationally agreed standards for blocking illegal sites (see advice below and the Links list)

Commercial Risks

Learners from 16 years of age are likely to have access to some kind of credit or debit card and be familiar with online purchasing. While they are with you they may see an opportunity to buy inappropriate content. They are vulnerable to phishing and other methods of identity theft. Training in appropriate actions to protect their personal data and education around issues of online scams can be embedded within tutorials, induction and citizenship.

Working across the partnership

For a list of resources for training around all of these issues, see the links section below. A dialogue between all partners in the consortium or 14-19 partnership will be needed to ensure that appropriate training is in place. It is worth working through the following questions with partners and then using the appropriate checklist across the partnerships with groups of staff. It's very important to develop a shared understanding of where learners might receive mixed messages, so that staff across the partnership can present a consistent approach.
Becta is working with Local Children's Safeguarding Boards to develop their policies on Safeguarding Online. LSCBs should have a Further Education presence; find out who is representing your partnerships in this way, and talk to them.

The next section gives some of the key questions you should be asking of yourself, your staff and your learners. Following this is a series of Checklists that you can work through with appropriate staff.

Some key questions for identifying hazards when working with young learners using technology or online

A Technology Audit

What technologies are used? Where? Who uses them?
What control do you as a learning provider or employer have over these technologies?
Do you own the technology and the connection, or are there instances where young learners may be communicating online using their own equipment?
What filtering and blocking technologies are in place?
How effective are these?

Are acceptable-use policies (AUPs) in place?

Do they cover all service users and all technology uses?
Are they appropriate to the age of the users?
Are users (or their designated parent/carer) required to sign the policy?
How is the impact of the AUP monitored?
Are processes in place for reviewing and updating the policy in line with developments in new technologies?
How are breaches of the policy identified and recorded?
What actions are taken when a breach occurs?

Are technical staff aware of the issues?

Is there regular dialogue with teaching staff about requirements for technology configuration to support the curriculum and individual learners as needed?
Are they fully aware of their proactive and reactive responsibilities for monitoring the network infrastructure in relation to safe working online?

Is your Risk Assessment for technologies adequate?

Are all staff involved as appropriate, including assessor, training co-coordinator, mentor, supervisor etc.?
Is the use of technology and risk assessment embedded within course planning?
Are lines of responsibility clear?
Are you up to day with the latest trends in technology use by your learners?
Are you talking to your learners regularly about their use of technology?

What do to first

In terms of **filtering**, learning providers should, as a **minimum**, use an Internet Service Provider or filter provider that subscribes to the Internet Watch Foundation's URL filtering list (see links below). URLs on that list contain potentially illegal content of child sexual abuse, but do not include potentially illegal content inciting racial hatred or any other inappropriate content. Additional filtering mechanisms must be employed to limit these risks, as appropriate to the users of the services in question. If your connection is provided through JANET then there are basic levels of filtering that you can control as needed.

Wireless networks should be secured and computers should be installed with anti-virus and spyware software and kept updated. Becta has an accredited provider scheme that lists ISPs and filtering products, some of which are available to work based learning or private learning providers.

A learning provider's **acceptable-use policy** (AUP) must be wide ranging. It must consider both fixed and mobile access to the internet, technologies provided by the service itself (such as PCs, laptops, webcams and digital video equipment) and technologies owned by service users and staff but brought onto the service premises (such as mobile phones, camera phones, personal digital assistants (PDAs) and portable media players). It should be flexible enough to deal with new and emerging technologies, but should also recognise the important educational and social benefits of such tools.
Additionally, the AUP should state what monitoring and reporting of individual usage is in place. Not only can this help to encourage a culture of safe and responsible behaviour, but also transparency of approach is important to alert users to their rights to privacy - which may help to avoid complications should safeguarding incidents occur. The AUP should include the security of the equipment being used. If PCs, laptops are not kept up to date with operating system updates and antivirus/spyware then users are vulnerable.
If you are accessing the internet through the JANET network then their AUP will apply, as will appropriate parts of the Home School Agreement that school-based learners will have signed when starting at their school. Your Local Authority may also have developed its own AUP. It would be worth looking at these to see how your systems can work with them and what further policies you may need to develop. You will need to talk to all your partnership partners about AUPs whether they are colleges, employers, private training providers. The development of a joint AUP can be a constructive focus for dialogue around the issues of Safeguarding.
Above all, involve your learners is dialogue about your AUP. Consider how you can use it as a vehicle for learning about working safely online, and increasing their skill level in ICT.

Further information on AUPs is available on the Becta website.

You should plan to **review the use of technology** within your organisation regularly – say every six months – to make sure that you are aware of any trends in usage and issues that have arisen and how they are being dealt with.

The following section breaks down some of these points to help members of staff think about the issues. They are categorised as roles that staff may have in your learning provider but it's important to have every member of staff aware of any risks – and the benefits - associated with the use of technology to enhance your business and the learners' experience with you.

Adult learners and staff may benefit from the wide range of training in learning with technology that is listed on the Becta web site and the QIA gateway. Some useful links are given below.

For further information please contact the Becta Further Education team at XXXX

A Checklist for Learning Providers

Policy issues for Managers

Have you decided whether to allow young learners to use your network?
What about bringing their own electronic devices into your organisation for use in training/tutorial sessions?

Do you have a named senior manager responsible for safeguarding online issues in your organisation?

Do you have clear lines of communication and responsibility set up between your organisation, employers, the home provider and the learners' parents or carers?

Do you have an Acceptable Use Policy for learners, and one for staff? Is it appropriate for younger learners, particularly those under 16? Does it contain clear sanctions if terms are breached? How do you know the learners have accepted its terms?

Do you have internet usage monitoring in place, so that you know who has used the internet and when?

Infrastructure Issues for Technical Team, Learning Delivery team and Managers

Do you have adequate filtering and monitoring software in place to safeguard younger learners? Is it linked to their log-in so their use can be monitored?

Are you allowing appropriate access to learning materials and on-line collaborative tools in dialogue with staff who are involved in delivering learning?

Are you allowing staff to have appropriate controls over the system so they can moderate learners' access as required?

Have you enabled your learners to access their home provider's system from your organisation?

Have you enabled your learners to access your organisations network/virtual learning environment remotely and therefore considered the security issues?

Education Issues for Curriculum/Programme Managers and Learning Support staff

Do you have a structured induction to your IT systems and acceptable use, perhaps as part of general learner induction to your organisation? In a 14-19 partnership, who is ensuring that the learner is inducted to all the technologies they will use?

Do you know about your learners? Do they have any learning needs, disabilities or social needs that may impact upon their use of technology? Is there any way technology can be deployed to help them learn about safe working online? Is there any expertise they have that you can tap into?

Have you embedded aspects of safe and responsible online working into the curriculum, for example in functional skills, tutorials or citizenship sessions?

Who is responsible for ensuring that each learner understands their rights and responsibilities whilst using technology in your organisation?

Are you confident in your control over the system you are using with learners and that you can access technical support as needed?

Glossary – a few selected terms; for more, see links list below

AUP Acceptable Policy (see Appendix for example)
A policy that a user must agree to abide by in order to gain access to a network or the internet. It should also consider how other communications devices, such as mobile phones and camera phones, can be used on the premises.

Blog
A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors

Buddy list
A buddy list appears in a window that shows all friends, family, co-workers, and others who are signed on to AOL, CompuServe (CS2000), and Instant Messenger Service (IMS) etc.

Filter
A method used to prevent or block users' access to unsuitable material on the internet.

Firewall
A network security system used to restrict external and internal information traffic .

Hacking
The process of illegally breaking into someone else's computer system, breaching the computer's security.

Internet service provider (ISP)
A company providing a connection to the provider internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

IWF
The Internet Watch Foundation is the only recognised non statutory organisation in the UK operating an internet 'Hotline' for the public and IT professionals to report their exposure to potentially illegal content online.

JANET(UK) - originally a contraction of Joint Academic NETwork.
Government-funded computer network dedicated to education and research. The network also carries traffic between Colleges and many schools within the UK, although many of the schools' networks maintain their own general Internet connectivity. JANET(UK) will be providing the connectivity for the new National Education Network (see links).

Malware
Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse. For a video explanation and quiz see the TUC resource workSmart video on malware

Social Networking
Sites like My Space, Bebo, and Facebook that allow users to upload images and messages and to form networks of contacts or 'buddies'.

Peer2Peer (P2P) networks
Peer-to-peer (P2P) network allows connected users to exchange files by uploading and downloading between them. This is only one of several ways files are shared on internet. Currently being used by the BBC iPlayer service.

Phishing, Spoofing
Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practiced to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source

Profile
An easy-to-create webpage which contains personal information a user gives about themselves. It can include all kinds of information, and users can upload their favourite music, pictures and video clips to their profile for other users to view.

Video Communities
A Video Community allows individuals to upload video clips to an internet website to share with others.
The video host stores the video on its server, enabling others to view and interact with the videos and the person that posted the original video. The most popular is YouTube.

Links useful to FE & Skills providers
For learners

- BBC Webwise Internet Safety quizzes
- Lesson plans and resources from Netsmartz (USA)
- ThinkuKnow Digizen advice and resources

For parents

- Becta Next Generation Learning e-safety quiz

For staff at the learning provider:

- Get Safe Online advice for adults and small businesses
- DIUS/TUC toolkit workSMART Not Safe for Work?
- Internet Watch Foundation
- Child Exploitation and Online Protection centre
- European Schoolnet site overview of issues
- Post-16 Citizenship from the LSN
- Training in E-learning from the LSN
- Online Esafety Certificate at Level1 via the OCN
  SQA Internet Safety course
- Risks to Employers of 'Cyberslacking' (from Pinset legal firm)
- Useful Posters can be downloaded from Kent Police
- JISC Plagiarism advice service
- TASI website
- Online Security – easy to read site, based in Ireland, on aspects of security
- A presentation outlining the risks associated with the use of 'cyber communities' (from the USA) cited by Easton College

Look out for:

- The LSIS module on Safeguarding – available from January 09
- Resources on the Excellence Gateway
- Guidance from appropriate Trades Unions
- Advice from the DCSF, Home Office and DIUS (Safeguarding theme)

Appendix
Sample AUP Policy 1 from Wolverhampton Learning Partnership

Acceptable Use Policy

Learners

Definitions:

- "Service Users" refers to all of the registered users of my-iPlan (i.e. http://ilp.my-iplan.com). They include students, teachers, other school staff and Nord Anglia elearning personnel

1. my-iPlan is a closed area of the Internet. Most schools require that you have obtained the permission of your parent(s)/guardian(s) before you can be allowed to use the Internet.
2. You must only access those services you have been given permission to use.
3. Do not disclose your my-iPlan login username and password to anyone.
4. Do not make use of any my-iPlan login username or password other than your own.
5. Do not download, use or upload any material from the Internet, unless you have the owner's permission.
6. Under no circumstances, when using my-iPlan, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or schools. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any use which may be likely to cause offence.
7. Avoid any acts of vandalism on or to my-iPlan. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
8. The use of strong language/swearing is not permitted.

Failure to comply with these rules will result in one or more of the following:

1. A suspension, temporary or permanent, from your use of the my-iPlan
2. A letter informing your school of the nature and breach of rules
3. Appropriate sanctions and restrictions placed on your access to school facilities, to be decided by the Head of Year/Head of Department
4. Any other action decided by the Head and Governors of your school

Authorised adults

Definitions:

- "Service Users" refers to all of the registered users of my-iPlan (i.e. http://ilp.my-iplan.com). They include students, teachers, other school staff and Nord Anglia elearning personnel

1. Do not disclose your my-iPlan login username or password to anyone, other than the people responsible for running and maintaining the system.
2. Do not download, use or upload any material from the Internet which is copyright of others.
3. Under no circumstances, when using my-iPlan, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or schools. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any use which may be likely to cause offence.
4. Always respect the privacy of files of other Service Users.
5. Avoid any acts of vandalism on or to my-iPlan. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.
6. The use of strong language, swearing or aggressive behaviour is not permitted. Do not state anything which could be interpreted as libel.
7. Report any incident that breaches the Acceptable Use Policy to Nord Anglia eLearning XXXXXX or email XXXXXXX

Failure to comply with these rules will result in one or more of the following:

1. A suspension, temporary or permanent, from your use of my-iPlan
2. A letter informing your school of the nature and breach of rules
3. Any other action decided by the Head and Governors of your school

If you do not understand any part of this Acceptable Use Policy, you must contact us by email: XXXXXXX

Acceptable Use policy from a Stoke-on -Trent FE College

If YOU want to use the College network, remember this!

* The College computer network (including Internet access) is provided to assist you in your studies. To use it, you must agree to the College rules for use - and keep to them.
* Note that ALL network use is monitored and logged, and that if you break the rules you will be caught.
* E-mail - do not access e-mail AT ALL during lessons (unless it is part of the class work and you have been told to do so by your teacher). You must make clear that you do not speak on behalf of the College in any e-mails that you do send, particularly if using a College e-mail address.
* Internet - do not visit websites that are not relevant to your coursework or other college-related activities.
* Games - you may not play ANY games on the college network, be they on the Internet, downloaded from it or brought in on floppy disk/CD-ROM.
* Music - may only be downloaded or listened to if it is part of your coursework (e.g. if you are a music student or are creating multimedia presentations). Remember that copyright applies to all sound files, and it is your responsibility to ensure that you listen legally.
* Objectionable behaviour - you must not access or create any material that could cause distress or offence to another member of the College. This includes bad language, overt sexual references or derogatory comments about other individuals or groups of people.
* Passwords and User IDs must be kept secure and not told to ANYONE. You are responsible for any abuse of the system logged from your account. Do not attempt to find out anyone else's password.
* Downloads and Installations - no software of any kind may be downloaded or installed on any part of the college system. This includes such as 'screensavers' as well as executable programs.
* Food and Drink may not be consumed in computer rooms.

The College seeks to encourage all members of the College to make use of the Internet, Intranet and other computing facilities. In so doing, it is necessary to ensure that all those granted access to the College's computing facilities, and in particular Internet access via the College system, use the facilities in an ethical, lawful and responsible manner.

Reasons for a written Code
A written code is necessary to ensure that all users of College computer facilities are aware of their rights and responsibilities; and to provide a yardstick against which the behaviour of College members can be measured.

To whom does the Code apply?

This Code applies to any person wishing to make use of College computing facilities and Internet access, and acceptance of it is a requirement for the issue of access rights.

LGfL example AUP for staff contains these 2 bullet points:

- **I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.**

- **I will not engage in any online activity that may compromise my professional responsibilities.**