6. Barriers and risks

Barriers to exploiting social networking services within education

What prevents educators from exploring and, where appropriate, using social networking services?

- **Educators' confidence and experience**

Educators' enthusiasm for social networking services varies, but the UK, along with other countries, is still in the process of embedding technology within education to support personalised learning, engagement, inclusion, creativity and innovation[i]. However, much is being done to support the widespread adoption of mobile and Internet technologies to support effective blended learning delivery and equip educators to evaluate which technologies might best support specific learning and teaching objectives. Some uses of ICT are now commonplace within schools and colleges[ii].

Professional development programmes, advice and information for teachers have not necessarily kept pace with the emergence of new technologies and practices, particularly those that have become widespread and commonplace among learners[iii]. Educators may well be using social networking services themselves, but may not recognise the educational potential and opportunities for their learners, or understand the potential risks, both for themselves and their learners. Many educators do not use the Internet in the same way as many young people – as a ubiquitous, always-on extension of their physical space which, for young people, has always been around[iv].

- **Negative views of social networking services**

Parents and educators alike are understandably concerned about illegal and anti-social behaviour online. Recent media coverage of social networking services has tended to focus on the negative aspects of services, for example the presence of predatory adults who want to use services to contact and groom young people[v]. Illegal and inappropriate behaviour is an unfortunate fact of human societies, whether it takes place online or offline. However, over-emphasising these types of activity is not useful in supporting young people to recognise, manage and negotiate risk for themselves. Just as in the real world, we need to approach risk in an even-handed and realistic way in order to best manage it. Most responsible social networking services employ people to post-moderate anti-social activity, although it should be noted that the amount of information published means that services are reliant on users making reports.

This year the British monarchy launched its own YouTube channel, and the Queen broadcast her Christmas message online[vi], which might suggest that social networking services are regarded by the establishment as a legitimate and effective way to reach a national and international audience, as television was when the Queen's speech was first broadcast in 1957.

- **Blocking and filtering procedures within UK education**

Almost all state schools within the UK subscribe to a broadband connection and services through their local regional broadband consortia (RBC)[vii]. Filtering and blocking policies are

determined and varied by the RBC in consultation with their partner local authorities; educators and institutions can request that sites should be blocked or unblocked.

Colleges and some schools may also have internal procedures for requesting site blocking or unblocking. Many schools block social networking services, viewing them as either housing inappropriate content or being a waste of time, not recognising the ways in which social networking services can be valuable to students. This can make it difficult for staff to explore or experiment with sites, or to respond to reports of cyberbullying or other inappropriate activity by their learners taking place on such services.

Young people visit social networking services from home and other out-of-school locations. Many young people are also adept at finding ways around blocking and filtering software in order to visit the sites they find meaningful and useful.

- **Digital media literacy policy**

Digital media literacy is not taught across all UK schools. While the new QCA secondary curriculum introduces e-safety as a compulsory topic in Key Stages 3 and 4[viii], many other aspects of media literacy which cover issues of relevance to current uses of mobile and Internet technologies are absent or taught according to the interest of the individual teacher. In particular, there is currently no UK-wide agenda for technology, citizenship and social participation, or around data protection and data management issues, including those relating to copyright and file sharing.

- **Lack of straightforward risk evaluation and management tools**

Many schools understand the value of activities that take place outside the classroom. Taking learners outside the school premises requires risk evaluation and management. In a similar way, teachers and schools need straightforward risk-evaluation tools that they can apply to social networking sites and web-based services if they plan to use them with learners.

UKOLN's Risk Assessment For Use Of Third Party Web 2.0 Services briefing document (http://www.ukoln.ac.uk/qa-focus/documents/briefings/briefing-98) highlights some of the technical issues which need to be addressed, but the issues are not contextualised for use in a teaching environment.

As well as issues relating to data management and backup, a risk assessment could, for example, include students' understanding and management of permission settings, their understanding of site terms of use and any agreed behavioural guidelines, and rights management of the materials they use and create.

Using social networking services – the risks

The following list of risks is not exhaustive. The risks of using social networking services often overlap with issues that have been well addressed by existing e-safety advice and guidance, for example Childnet's award-winning Know IT All series of resources (http://www.childnet.com/kia).This list looks at risks that are specific or pertinent to social networking services. Educators should, however, have a general understanding of the benefits and risks of using technology.

- **Misunderstanding the nature of the environment**

Many users believe that they are writing for a closed group of friends, unaware that the information they have posted may be publicly available and able to be searched for and read by a much wider audience. Acquisti & Gross (2006) characterise social networking services as "imagined communities" in recognition of the gap between users' perceptions of a private, closed network and the reality of who can access their information[ix].

Additionally, it may not occur to young people that their public arguments or "flame wars", their overly enthusiastic critiques of their teachers, or the risqué pictures of themselves that seemed quite funny at the time may still be around in a few years when they are applying for a job or trying to get into university, for example.

We don't yet know the full consequences for a generation that has grown up online, or the future implications of new types of search, for example social searches, which aggregate information from across a range of social networking sites by your name or email address, or of the development of facial-recognition search software.

Managing the risks

Site members need to be mindful of what they post and how they behave publicly online. Anyone who wants to post pictures or videos of other people should ask for their permission. Service users should ensure they don't give out inappropriate or personal information/content about themselves or other people. Some services – for example, YouTube – require users to have the permission of the people appearing in videos before they post them.

In addition, service users should understand site permissions, for example privacy settings, and be able to use them effectively to regulate who gets access to the information they post. The granularity of site permissions varies from site to site, and some sites have very complex permissions available to users. Understanding how permissions work is important to all members, otherwise they may allow more people than they intend to see information, or make information available to public search engines.

Basic permissions will be some variation on "private", "friends", and "public". It is important to remember that private information isn't necessarily private from the service provider, so information sent via instant messaging or social networking services' mail should be thought of in the same way as postcards. Also, people who collect "friends" may end up making personal information available to people and networks that they don't really know or trust. Members who don't know and trust everyone on their friends list need to treat any information made available to "friends" in the same way as they would treat public information.

All Internet users need to think about all the information they post. This means not just thinking about the information they publish to one location or social networking service, but about all the information collectively over all the sites they use. Using search engines to search for themselves is an easy way of checking what information other people might find. Looking for specific information – such as a home phone number, photographs or a home address – can help users identify and take down inappropriate information, although making sure this kind of information is not posted in the first place is the most effective strategy.

Many social networks allow users to close accounts and permanently delete their information. It is important that users remember that publicly posted information may remain accessible

through Google cache records – which produce a copy of pages that have been searched – even after information has been taken down or deleted.

The law applies to social networking services as well as to anywhere else, and certain content and behaviours are illegal. In addition, services have their own rules in their terms and conditions. It is important that users are aware that they can report issues to the service provider and also to the police. It is good practice for service providers to have clear and accessible reporting functions available to their users.

When reporting, it is helpful if users keep evidence of what they want to report. For social networking services, keeping the URL, copying the relevant pages, or even printing the page can be useful ways of preserving evidence.

- **Controlling your data, and losing control**

It is important that educators can access the information and resources they have created online. Network issues affect access to the Internet. Most major services advertise downtime (for example when the service needs to close for maintenance or improvement), but services still occasionally become inaccessible. Service outage can be devastating if an educator plans a live demonstration of a site or has materials online for a due project or looming exam date.

Always make sure you have backup copies of essential documents, and think about alternative ways of using and storing your information. Carry out a simple risk assessment to check what you would do, for example, if the site goes down during exam week or if important data are lost or permissions reset.

- **Intruding on young people's space**

Using some social networking sites might be viewed as an intrusion on young people's personal space, especially if the permissions set is not granular enough to allow different functions between different kinds of groups or friends.

Investigate group functions; for example, if a member of staff wants to use a site to moderate or lead activities, it might be appropriate to find a site that doesn't require people to be friends to be members of the same group (i.e. that has an additional level of access permissions). Consider sites that your students don't have a personal attachment to, so that students can establish a professional account, and make sure that appropriate behaviour is discussed and negotiated before using the platform.

Another alternative is to provide information in an official or objective capacity, for example setting up an account or page as a group or a school, rather than as an individual. Again, you will want to look for a site that doesn't require reciprocal friendship, or enables your students to keep their personal information private.

- **Cyberbullying and anti-social behaviour**

Cyberbullying can be defined as the use of ICT, particularly mobile phones and the Internet, deliberately to upset someone.

It is vital that schools understand the issue (see http://www.digizen.org/cyberbullying/fullguidance/understanding), know how to prevent

incidents (see http://www.digizen.org/cyberbullying/fullguidance/preventing) and respond to incidents (see http://www.digizen.org/cyberbullying/fullguidance/responding), and keep up to date on the legal issues surrounding this challenging subject.

Make sure all your students understand what cyberbullying is and what the impact and consequences can be. For more information, see the guidance for schools on preventing and responding to cyberbullying that Childnet has produced for the Department for Children, Schools and Families (DCSF) (see http://www.digizen.org/cyberbullying).

Check also that students know how to identify and report inappropriate behaviour on sites they are using.

- **Impersonation and identity theft**

Everyone should understand that people online are not necessarily who they say they are. Someone may pretend to be a real person or invent a new identity. People might be dishonest about anything: their addresses, names, ages, genders or interests.

There are a broad range of reasons why someone might be untruthful. For example, fake profiles can be used to cyberbully or be used by an adult to groom children (see below for information about grooming).

There are risks related to giving out too much personal information publicly on social network services. One risk of giving out too much personal information is identity theft. There are also clear risks in giving out information which can enable others to contact and locate you offline.

- **Potentially illegal behaviour and illegal content**

Online grooming of a child is illegal in the UK. Online grooming refers to a number of techniques that are used to engage the interest and trust of a child or young person for the sexual gratification of an adult. An adult makes contact with a child in an online environment, then develops a relationship with the child, manipulating the child's emotions with the intention of arranging a meeting and sexually abusing the child. People who do this often lie to gain trust, and may or may not pretend to be someone else. They may also try to use either threats or guilt to try and secure a meeting with the child or young person.

Any suspected potentially illegal activity with a child or young person online can be reported to the UK's Child Exploitation and Online Protection Centre (CEOP) (http://www.ceop.gov.uk).

Illegal content in the UK includes indecent images of children, material that incites racial hatred, and criminally obscene content. Potentially illegal content can be reported to the UK's national hotline, the Internet Watch Foundation (http://www.iwf.org.uk). It is important that young people who post pictures of themselves or their friends online think about the appropriateness of these images, and are aware that indecent images of children (i.e. people under 18) are illegal.

- **Sites or services spamming address books or contacts lists**

Users should be careful when they sign up to anything that involves giving access to an address book. Unscrupulous sites may spam contacts, for example inviting them to join services in order to boost their membership. While it may be useful to search for those among your contacts/address book using the same service, it is important for users to understand what they are agreeing to allow the service to use that information for.

- **Don't be bullied into being "friends" with someone**

For social networking service users, deciding whether to accept a new "friend" can be socially difficult. However, users should never feel bullied into accepting people. Accepting a "friend" and then later trying to delete that person from a friends list without anyone noticing is not a good strategy, although users should remove and block people when necessary, and report to the provider any people who have broken the service's terms of use.

Users should decide a clear framework for accepting "friends". The rules chosen may vary from service to service; for example, users may decide to use a service account as a very public one and accept "friendship" from anyone who offers it. Alternatively, users might decide only to accept requests from people they know reasonably well, or from people they regard as close friends. Users should always ask people requesting friendship where they know each other from, if they don't remember.

---

[i] Department for Children, Schools and Families (2005) Harnessing technology: Transforming learning and children's services. March. Retrieved 20 February 2008 from http://www.dfes.gov.uk/publications/e-strategy

[ii] Becta (2007) Harnessing technology review 2007. September. Retrieved 20 February 2008 from http://partners.becta.org.uk/index.php?section=rh&catcode=_re_rp_02&rid=14409

[iii] Becta (2006) Emergent technologies for learning. January. Retrieved 20 February 2008 from http://publications.becta.org.uk/display.cfm?resID=25940&page=1835

[iv] Prensky, M. (2001) Digital natives, digital immigrants. On the Horizon, 9(5), October. Retrieved 20 February 2008 from http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

[v] Bahney, A. (2006) Don't talk to invisible strangers. The New York Times, 9 March. Retrieved 20 February 2008 from http://www.nytimes.com/2006/03/09/fashion/thursdaystyles/09parents.html

[vi] The Royal Channel: http://www.youtube.com/theroyalchannel

[vii] The National Education Network: http://www.nen.gov.uk

[viii] National Curriculum: http://curriculum.qca.org.uk

[ix] Acquisti, A. & Gross, R. (2006) Imagined communities: Awareness, information sharing, and privacy on the Facebook. Retrieved 20 February 2008 from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf