Simple Guidance for Staff in Education Settings on the Use of Social Network Sites

January 2012

OXFORDSHIRE COUNTY COUNCIL
CHILDREN AND YOUNG PEOPLE'S DIRECTORATE

GUIDANCE ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA

Introduction

The aim of this document is to provide some simple advice and guidance for those working with children and young people in educational settings (including volunteers) regarding the use of social Networking Sites.

The document has been produced for Governing Bodies and Head teachers of all Schools in Oxfordshire and for Senior Managers and Management Committees within the County Council's centrally managed teaching services.

Background

The use of social networking sites such as Facebook, Bebo and MySpace is rapidly becoming the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube and blogging sites.

It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits.

It is naïve and out-dated however to believe that use of such sites provides a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

Difficulties arise when staff utilise these sites and they do not have the knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

Specific Guidance

Employees who choose to make use of social networking sites/media should be advised as follows:

- That they familiarise themselves with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended. We would recommend that as a minimum all privacy settings are set to friends only, irrespective of use/purpose

- That they do not conduct or portray themselves in a manner which may:
  - Bring the school into disrepute;
  - Lead to valid parental complaints;
  - Be deemed as derogatory towards the school and/or its employees;
  - Be derogatory towards pupils and/or parents and carers;
  - Bring into question their appropriateness to work with children and young people.

- Before using any social networking site to communicate with parents, carers or children that this is agreed with the school's leadership team

- That they do not form on-line 'friendships' or enter into communication with parents/carers and pupils as this could lead to professional relationships being compromised.

- On-line friendships and communication with former pupils should be advised against, particularly if the pupils are under the age of 18 years

(In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to the Specific Guidance points above).

Safeguarding issues

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messages can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young People in Educational Settings (March 2009)" states:

"12. Communication with Pupils (including the Use of Technology)

In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that e.safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online guidelines on acceptable user policies. These guidelines detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential."

This means that schools/services should:

- Have in place an Acceptable Use Policy (AUP);
- continually self-review E-Safety policies in the light of new and emerging technologies;
- have a communication policy which specifies acceptable and permissible modes of communication.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messages, e-mails, digital cameras, video, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request or respond to any personal information from the child/young person other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

This means that adults should:

- ensure that personal social networking sites are set at private and pupils are never listed as approved contacts;
- never use or access social networking sites of pupils;
- not give their personal contact details to pupils, including the mobile telephone number;
- only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used;
- only make contact with children for professional reasons and in accordance with any school/service policy;
- recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible;
- not use the internet or web-based communication channels to send personal messages to a child/young person.

Adults should be circumspect in the communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-

mail or text communications between an adult and a child/young person outside agreed protocol may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internet e-mail systems should only be used in accordance with the school/service's policy.

Further information can be obtained from
http://www.education.gov.uk

Recommendations

1. That this document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.
2. That appropriate links are made to this document with your school/services Acceptable Use Policy.
3. We would require that your school ICT policy makes clear the expectations on use of social network sites for staff and ideally set some boundaries around use including times of use and whose computer is used.
4. That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites.
5. The employees are informed that disciplinary action may be taken in relation to those members of staff who choose not to follow the Specific Guidance outlined above.

FAQ

Q1. Should I use my mobile phone to take photographs or video of students?

A. School trip is a common situation where photography by pupils and staff should be encouraged, but there are potential dangers.

The safest approach is to avoid the use of personal equipment and to use a school-provided item. One potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to prove that this was not the case. With school equipment there is at least a demonstration that the photography was consistent with school policy. Please also refer to the Oxfordshire Guidance of Taking Photographic Images of Children. Care should also be taken that photographs are stored appropriately. For instance to copy the photographs onto a personal laptop as opposed to a school allocated laptop might make it difficult to retain control of how the picture is used. Memory cards, memory sticks and CDs should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the school network, images should be erased immediately from their initial storage location.

It is important to continue to celebrate achievements of pupils through the appropriate use of photography in communicating with parents and the community.

Q2. Should I continue to use my Social Networking site?

A. Social networking is a way of life for most young people and many adults. However, adults working with children and young people should review their use of social networks as they take on professional responsibilities. Strong passwords should be used and security settings should be applied so that you control all access to your profile.

Information once published, e.g. photographs, blog posts etc is impossible to control and may be manipulated without your consent, used in different contexts or further distributed. Some adults have been caught out by posting amusing remarks about the school or colleagues, only to find them re-published elsewhere by their “friends”. Even innocent remarks such as an interest in “Gang Wars” could be misinterpreted (this is actually a game).

False social networking sites have been set up by pupils and staff with malicious information about staff.

Currently only a few public social networking sites authorise their members and use automated registration systems, which provide limited checks.

Social networking is an excellent way to share news with family and friends. Providing the security levels have been set correctly and a strong password

used, information should remain private. The danger is that few people understand profile privacy settings. The minimum age of use of a social networking website must be observed by a school, even though many pupils disregard this legal requirement.

Some instant messaging applications such as MSN have a facility to keep log of conversations, which could be used to protect staff in case an allegation is made.

“Don’t publish anything that you would not want your mum, children or boss to see, either now or in ten years’ time!”

“Think before you Post” (National Centre for Missing or Exploited Children)

Q3. Should I have my pupils as friends on instant messaging services?

A. Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child/young person other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Online communication provides excellent opportunities for collaborative work between groups of pupils. Monitoring or tuition, where appropriately arranged, could guide and enhance such activities.

Consideration should be given as to how this type of communication might appear to a third party. Compared with a conversation in school the use of new technology inevitably increases the potential for messages to be seen out of context or misinterpreted.

If instant messaging and other social networking sites are to be used with pupils, a separate and approved account should be set up for this purpose, with the agreement of senior management.

Staff need an online environment which is under their control. The first requirement is that you know who you are talking to; users must be authenticated. Schools and Local Authority should have a range of security features available to them. Logs should be available in case a false allegation is made.

Q4. What is my responsibility for the use of my school laptop at home?

A. Things that can go wrong include:

- Access to wider sites by family members, for instance a gaming site or internet shopping would increase the possibility of virus attack and identity theft.

- If another member of the family or a friend is allowed to use the computer it is difficult to ensure that the use has been appropriate, for instance that confidential information has not been accessed. Adults vary enormously in their judgements as to what is appropriate.
- If a school laptop is used at home for personal use, then it may be a taxable benefit.

Some adults may feel that access via a school laptop to adult material outside school hours and at home is appropriate. It is not; there is always a possibility that this material might be accidentally seen by a child/young person and in some cases this type of use has led to dismissal.

Adults need to remember that in order for anyone else to use a school laptop in the home setting, they would need to be logged on by the person responsible for the laptop. With this in mind, think about who would be culpable in certain situations.

Personal use of technology by adults has been shown to increase competence and confidence and should therefore be encouraged.

Adults should refer to the school policy on the personal use of school laptops, which unfortunately varies between school and between local authorities. Increasingly the use of a school computer for non-professional use is being explicitly banned.

"There are no circumstances that justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to the children". (DCSF Nov 2007) Adults should therefore ensure that they must have absolute control of a school laptop allocated to their use.

Q5. What is inappropriate material?

A. Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate' and 'illegal' and 'inappropriate' but 'legal'. All staff should be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Illegal

Possessing or distributing indecent images of a person under 18 – viewing such images on-line may well constitute possession even if not saved. What is regarded as indecent would ultimately be down to a jury to decide. The police

have a grading system for different types of indecent images. Remember that children may be harmed or coerced into posing for such images and are therefore victims of child sexual abuse.

Hate/Harm/Harassment

General: There is a range of offences to do with inciting hatred on the basis of race, religion, sexual orientation etc.

Individual*:* There are particular offences to do with harassing or threatening individuals – this includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Inappropriate

Think about this in respect of professionalism and being a role model. The scope here is enormous, but bear in mind that "actions outside of the workplace that could be as serious as to fundamentally breach the trust and confidence placed on the employee" may constitute gross misconduct.

Examples taken from real events:

- Posing offensive or insulting comments about the school on Facebook.
- Accessing adult pornography on school computers during break.
- Making derogatory comments about pupils or colleagues on social networking sites.
- Contacting pupils by e-mail or social networking without senior approval.
- Trading in sexual aids, fetish equipment or adult pornography.

Q6. **How should I store personal data safely?**

A. Teachers often find it convenient to write pupil reports or staff appraisals and references at home. This may require access to confidential personal information.

B. All personal information must be kept secure. The storage of data on a hard disk or other means is basically insecure. Making such storage secure may include password protection, encryption of data and locking the computer when not in use. Physical risks including mislaying a memory stick and laptop theft from a vehicle are all too common. Consider approaches such as not storing information unless necessary and deleting files after use. The safest long-term storage location may be the school network, which should have a remote backup facility.

“Information security is an integral part of the Data Protection Act 1998. You must take all reasonable steps to ensure that any personal information that you are processing is securely stored.”

All staff are strongly advised to ensure that they understand their school policy regarding data protection. National policy is developing rapidly in this area. To lose control of personal data while not complying with the school policy would be difficult to defend.

Q7. How can I use ICT appropriately to communicate with young people?

A. Young people are encouraged to report concerns, which may involve the use of new technology, e.g. a pupil might prefer to text a report about bullying, rather than arrange a face to face discussion.

Friendly verbal banter between adult and pupil may not be inappropriate, but it might look very different if carried out via E-mail or MSN and might lead to difficulties if misinterpreted, forwarded or used out of context. Care in the use of automatic signatures is required e.g. “Sexylegs” is not an appropriate signature for either pupil or adult when in an educational setting.

Adults should be aware of, and comply with, the school policy on the use of text or MSN.

“Adults should be circumspect in their communications with children and young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.” (DCSF Nov 2007).

Q8. As a teacher, how can I safely monitor school network use?
Filtering or recording network usage will only be effective if monitored carefully to notice and report inappropriate access or usage. Often this places a new responsibility on technical staff that they may not be trained for. This responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity.

A. It is wrong to assume that filtering and monitoring are simply technical ICT activities solely managed by the network staff. Some technical staff have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial. However technical staff should not be expected to make judgements as to what is inappropriate material or behaviour without support and supervision. Monitoring policy must be set by the senior leadership team, with set procedures to deal with incidents. The senior leadership team will require assistance from technical staff but must also involve the school designated child protection coordinator and pastoral staff.

A technician might, with the best of intent, check sites that a user has visited and email images to alert a colleague. Should the images prove to be illegal the technician has committed a criminal offence. A defence may be that the

technician was acting within a published school procedure but staff should ensure that they receive a specific, written request to perform this work.

Should an incident of concern occur there should be a clear route for immediate reporting to a senior leader. Procedures to preserve evidence by unplugging a computer or locking an account need to be in place.

Q9. Can my school limit private on-line publishing?

A. As a teacher I have been asked to sign a "Professional Conduct Agreement" that requires me to be careful when using ICT out of school. Surely that is my own business?

One situation included a teacher complaining about a parent's rudeness. Had the conversation remained private as no doubt intended, this might be regarded as simply letting off steam. However, because a social networking site was used with incorrect privacy settings, an unintended audience was included and a complaint made.

The situation is not new; teachers discussing a pupil in a shop queue might be overheard by a parent. However the technology enables messages to be recorded, edited maliciously, used out of context, re-published or used as evidence.

The mode of use of social networking and instant messaging is often conversational with a rapid interchange of remarks. It is easy to stray from a non-school conversation between friends to professional matters and perhaps not realise the lack of control over audience.

The teacher should either be fully conversant with the security arrangements for the site in use or better avoid any information that could compromise their professional integrity.

Q10. How do I ensure safer online activity in the primary classroom?

A. Most internet use in schools is safe, purposeful and beneficial to pupils and staff. However there is always an element of risk; even an innocent search can occasionally turn up links to adult content or imagery.

Planning and preparation is vital and the safest approach when using online material in the classroom is to test sites on the school system before use. For younger pupils you should direct them to a specific website or a selection of pre-approved websites and avoid using search engines.

When working with older pupils, select appropriate and safe search engines e.g. CBBC Safe Search. Appropriate search terms should be used and pre-checked. Consider carefully the age, ability and maturity of all pupils when planning online activities.

When encouraging pupils to publish work online, schools should consider using sites such as “Making the News”, Microsites (hosted by SEGfL), video hosting sites such as SchoolsTube and TeacherTube and virtual learning environments. For image searching use sites such as Microsoft Clip Art Gallery and the National Education Network Gallery.

If inappropriate material is discovered then turn off the monitor, reassure the pupils and to protect yourself you need to log and report the URL to a member of the senior leadership team according to the school’s E-Safety policy. Avoid printing or capturing any material.