

Safer Practice with Technology

For adults working in schools



Using technology as a communication tool in professional relationships

Protecting adults from misinterpretation of behaviour

Understanding personal and professional boundaries

Safer use of Electronic Media

Inappropriate & Illegal Material

Portable Devices

YouTube

Mobile Phones

Social Networking

Safer Search



Unisys, the supplier of the KPSN broadband network, has kindly covered the costs of printing this booklet.

Contributory authors:

Rebecca Avery, CFE; Peter Banbury, EIS; Heidi Barton, ASK; Martin Carter, Kent Police; Rachel Keen, SENICT; Carolyn Lewis, ASK; Steve Moores, Maidstone Grammar School; Mike O'Connell, Child Protection; Andy Place, ASK; Marc Turner, EIS; Carol Webb, Invicta Grammar School; Pam Wenban, Riverview Junior School.

May we also thank the following and their colleagues in compiling and testing this booklet?

Patrick Kirk and Victoria Clapham, Leeds Learning Network; Jacqui Moore and Zoe Barkham, Medway Council; Ruth Hammond, Becta.

This booklet will evolve as new questions are added and answers improved with experience. Please submit any comments to the editors:

Rebecca Avery,
e-Safety Officer, KCC schools.
rebecca.avery@kent.gov.uk

Peter Banbury,
Chair, Kent Schools e-Safety Strategy Group.
peter.banbury@kent.gov.uk

Use of this material

The copyright of this material is held by Kent County Council. However educational agencies are hereby granted permission to use all or part of the material for not for profit educational use, providing the KCC copyright is acknowledged.

The latest version is available at
www.kenttrustweb.org.uk?esafety

Safer Practice with Technology

May 2009

This document responds to questions raised by adults working with children and young people. Adults in this area of work need to ensure they are competent, confident and safe when working with new technology.

All adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust. This document discusses appropriate and safer behaviours for adults working in paid or unpaid capacities, in a school context.

A rules approach cannot resolve such complex issues. This booklet suggests a set of real situations to enable adults to develop greater awareness of the dangers and to consider consequences of behaviour earlier in a developing situation.

This document aims to:

- Assist adults to work safely and responsibly and to monitor their own standards and practice.
- Help adults to set clear expectations of their own behaviour and to comply with codes of practice.
- Minimise the risk of misplaced or malicious allegations being made against adults.
- Project a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary action will be taken.
- Support managers and leaders in establishing a culture which safeguards staff and young people in their organisation.

Based on “Guidance for Safer Working Practice for Adults who work with children and Young People” DCSF Nov 2007 [*See Links 1*].

Frequently Asked Questions

- Q1** Should I use my mobile phone to take photographs of students?
- Q2** Should I continue to use my Social Networking site?
- Q3** Should I have my pupils as friends on Instant Messaging services?
- Q4** What is my responsibility for the use of my school laptop at home?
- Q5** What is inappropriate material?
- Q6** How should I store personal data safely?
- Q7** How can I use ICT appropriately to communicate with young people?
- Q8** As a technician, how can I safely monitor school network use?
- Q9** Can my school limit private on-line publishing?
- Q10** How do I ensure safer online activity in the primary classroom?

If in doubt

- Consult with your line manager and school policies.
- Consider how an action would look to a third party.
- Only publish content that you would be happy to share with parents, pupils and your employer.

Using this document

- Provide copies when staff sign their establishment’s Acceptable Use Policy.
 - Organise a staff development session around these questions.
- Add this guidance to the staff induction pack and place in staff areas.

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

- A. 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 Kent Guidance on the Use of Photographic Images of Children [See *Links 2*]

Care should also be taken that photographs are stored appropriately. For instance to copy the photograph on to a personal laptop as opposed to a school allocated laptop might make it

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

difficult to retain control of how the picture is used. Memory cards, memory sticks and CD's 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.

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 their school or colleagues, only to find them re-published elsewhere by "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.

.....
Social networking is an excellent way to share news with family and friends. Providing the security of your profile has 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 site must be observed by a school, even though many pupils disregard this legal requirement.

Currently few public social networking sites authenticate their members and use automated registration systems which provide limited checks.

Some instant messaging applications such as MSN have a facility to keep a 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!” Anon

“Think before you Post” National Centre for Missing or Exploited Children [*See Links 3*].

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

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

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.” (DCSF Nov 2007), [*See Links 1*]

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. A Local Authority provided or recommended communication and collaboration area will have a range of security features set within a policy framework. 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

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

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.

Adults should refer to the school policy on the personal use of school laptops, which unfortunately varies between schools 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 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 image. 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 so serious as to fundamentally breach the trust and confidence placed in the employee” (SPS 2004) may constitute gross misconduct.

Examples taken from real events:

- Posting 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 email or social networking without senior approval.
- Trading in sexual aids, fetish equipment or adult pornography.

The Schools e-Safety Policy 2007 provides more information in section 5, page 34. [*See Links 4*]

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.

All personal information must be kept secure. The storage of data on a hard disk or memory stick and transfer by email 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.” Please refer to the Kent Records Management Toolkit for Schools. [*See Links 5*]

All staff are strongly advised to ensure that they understand the school policy regarding data protection. National policy is developing rapidly in this area [*See links 6*]. 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 email 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 education 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).

Schools should consider carefully whether staff should use their personal email addresses or phone numbers to communicate with young people.

In all cases ensure that your relationships with young people are known and approved by the Senior Leadership Team.

Q8 As a technician, 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.

The flowchart produced by the Kent Children Safeguards Service will guide the schools response to an incident of concern. [*See Links 7*]

Q9 Can my school limit private online publishing?

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?

- A. 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 an appropriate and safe search engine 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 the Microsoft Clip Art Gallery and the National Education Network Gallery. [*See Links 8*]

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 schools e-Safety policy. Avoid printing or capturing any material.

Questions for Discussion

These might be used to initiate further staff discussion:

- Can I use a school computer to book holidays etc during lunch time or after school?
- How can I avoid infringing copyright law when using materials obtained online?
- How should I respond if I am subjected to cyber bullying by pupils?
- Can I respond to a comment about the school on the Friends Reunited site?
- May I use Bebo with year 8 pupils to discuss a history topic?
- Should I text a pupil in the evening to remind him to provide some useful Internet links and encourage him to complete a project?
- How should I research Nazi sites to produce a lesson for sixth form pupils?
- Should my year six pupils use a search engine?

Links

1. **Guidance for Safer Working practice for Adults who work with Children and Young People** (DCSF November 2007)
www.kenttrustweb.org.uk/Children/safeguards_policy.cfm

2. **Guidance for Kent Schools and Services on the Use of Photographic Images of Children**
www.kenttrustweb.org.uk/docs/child_safe_photo_guidance.doc

3. **National Centre for Missing or Exploited Children**
www.cybertipline.com

4. **Kent Schools e-Safety Policy and Guidance 2007**
www.kenttrustweb.org.uk?esafety

5. **Kent Records Management Toolkit for Schools**
www.kenttrustweb.org.uk/Policy/dpfoi_recman.cfm

6. **Becta: Good practice in information handling in schools: Keeping data secure, safe and legal**
http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf

7. **Flowchart for handling an Incident of Concern**
www.kenttrustweb.org.uk/Children/safeguards_policy.cfm

8. **National Education Network**
www.nen.gov.uk

General e-Safety Links:

A booklet on e-safety links may be downloaded from the Schools' e-Safety site:
www.kenttrustweb.org.uk?esafety.



Contact Information

Schools e-Safety Officer
esafetyofficer@kent.gov.uk

KPSN Schools Broadband
The EIS Centre
Oxford Road,
Maidstone,
Kent
ME15 8AW

Tel: 01622 683708



Designed and printed by EIS
01622 683708



Safer Practice with Technology

For adults
working in schools