KENT SAFEGUARDING CHILDREN BOARD

KSCB

SAFEGUARDING THE CHILDREN OF KENT

Safer Practice with Technology

Guidance for adults who work with children and young people

Document Name & File Location	K:\SS Service Policy & Standards - C&F\KSCB\Policy & Procedures	
Document Author	Kent Safeguarding Children Board E-safety Sub-group	
Document Owner	Kent Safeguarding Children Board © Sessions House County Road, Maidstone. Kent. ME14 1XQ Email: kscb@kent.gov.uk	
Copyright ©	The copyright of this material is held by the Kent Safeguarding Children Board. However agencies are hereby granted permission to use all or part of the material for not for profit safeguarding use, providing the KSCB copyright is acknowledged. The latest version is available at http://www.kenttrustweb.org.uk?kscbpolicy	
Summary of Purpose	Communication between children 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 messaging, e-mail, digital cameras, videos, webcams, websites and blogs. This document responds to questions raised by adults from various settings in this area to ensure that they are competent, confident and safe when communicating with children and young people.	
Review date	This booklet will evolve as new questions are added and answers improved with experience. Please submit any comments to the Kent Safeguarding Children Board at kscb@kent.gov.uk	
Accessibility	This document can be made available in large print, or in electronic format. There are no copies currently available in other languages	
How this document was created	**Draft 1**	Document created by E-safety Group
	Draft 2	Consultation with stakeholders
	Draft 3	Approval by KSCB
Equalities Impact Assessment	During the preparation of this annual report and when considering the roles and responsibilities of all agencies, organisations and staff involved, care has been taken to promote fairness, equality and diversity in the services delivered regardless of disability, ethnic origin, race, gender, age, religious belief or sexual orientation. These issues have been addressed in the policy by the application of an impact assessment checklist.	
Circulation Restrictions	Public Policy Document at Draft 3	

Version	**Detail of change**	**Date**
1.0	Document Created	March 2010
2.0		
3.0		

Safer Practice with Technology

January 2010

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 safe behaviours for adults working in paid or unpaid capacities with children and young people.

The Kent & Medway Safeguarding Children Procedures 2009 [*See Links 1*] should be followed at all times. 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:

- Ensure safeguarding children in the digital world is a priority.
- 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 allegations being made against adults about inappropriate behaviour.
- 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 that 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 Jan 2009 [See Links 2]*

Frequently Asked Questions

Q1 Should I use my mobile phone to take photographs of children or young people?

Q2 Should I continue to use my social networking site?

Q3 Should I have children or young people as friends on instant messaging services?

Q4 What is my responsibility for the use of my work 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 organisation limit private online publishing?

Q10 How do I ensure safer online activity in a hospital classroom?

If in doubt

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

Using this document

Provide copies when staff sign their organisation's Acceptable Use Policy
Organise a staff development session around these questions
Add this information to the staff induction pack and place in staff areas

Q1 Should I use my mobile phone to take photographs or video of children or young people?

A. A residential home or sports event is a common situation where photography by children and young people and staff should be encouraged, but there are potential dangers.

The safest approach is to avoid the use of personal equipment and to use an organisation or agency 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 organisation equipment there is at least a demonstration that the photography was consistent with the organisation's policy. Please also refer to the Kent Guidance on the Use of Photographic Images of Children [*See Links 3*].

Photographers should ask for permission to take a photograph to ensure compliance of the Data Protection Act. They should also get consent from parent, carer or guardian; see www.ico.gov.uk. In each case the consent of senior managers should be given before taking images or videos of children and young people. Care should also be taken that photographs are stored appropriately. For instance, to copy the photograph onto a personal laptop as opposed to a work allocated laptop might make it difficult to retain control of how the picture is used.

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

Secure memory cards, memory sticks and CDs provided by work should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the organisation's network images should be erased immediately from their initial storage location.

It is not appropriate to amend or manipulate the images (exceptions may be to brush out a school badge to protect identity or to crop a picture to fit).

Q2 Should I continue to use my social networking site?

A. Social networking is a way of life for many young people and 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 or privacy settings should be applied so that you can control all access to your profile.

Once published, information such as photographs and blog posts are almost impossible to control and could potentially be manipulated without your consent or knowledge, used in different contexts or distributed. Some adults have been "caught out" by posting comments or remarks about work or colleagues only to find them republished elsewhere. Even joining an online game or application such as "Gang Wars" could be misinterpreted.

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 organisations, even though many young people disregard this legal requirement.

False social networking sites have been set up by young people, parents/carers and even colleagues with false or malicious information about staff. Currently, few social networking sites authenticate their members offline and generally they use automated registration systems which can only provide limited checks.

Some instant messaging applications (such as MSN) have a facility to record 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 4*)."

Q3 Should I have children and young people 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." (DCSF Jan 2009), [*See Links 2*]

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

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

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.

Personal e-mail addresses, instant messaging identities, social networking accounts or telephones (fixed or mobile) should never be used to contact children or young people without the explicit agreement of the line manager. A separate professional account or contact should be used and this agreement MUST be formally recorded.

Staff need an online environment that is under their control. The first requirement is that you know who you are talking to; users must be authenticated. An organisation 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 work 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. Adult judgement varies enormously on what is appropriate.

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

If a work laptop is used at home for personal use, then it may be a taxable benefit.

Some adults may feel that access via a work laptop to adult material outside working hours and at home is appropriate. It is not; there is always a possibility that this material might be accidentally seen by a child or 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 work laptop in the home setting, they would need to be logged on by the person responsible for the laptop. With this in mind, misuse of that laptop is likely to rest with the designated user of the laptop.

Adults should refer to the establishment policy on the personal use of work laptops, which unfortunately varies between organisations and local authorities. Increasingly, the use of a work computer for non-professional purposes 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 Jan 2009)

Adults should therefore ensure that they must have absolute control of a work 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

Accessing (viewing), making, storing (possessing) or disseminating indecent images of children on or off the internet, whether on or off work premises is illegal. If proven this will lead to criminal proceedings and the individual will be barred from working with children and young people (IRSC 2006). Sharing adult pornography with children is also illegal.

Possessing or distributing incident images of a person under 18 can include viewing such images online. This may also constitute possession even if they are not saved. What is regarded as indecent would ultimately be a jury's decision. 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 as 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 organisation/agency on Facebook.
- Accessing adult pornography on work computers.
- Making derogatory comments about children or young people or colleagues on social networking sites.
- Contacting children or young people you work with by email or social networking without senior approval.
- Trading in sexual aids, fetish equipment or adult pornography.

Q6 How should I store personal data safely?

A. Staff often find it convenient to write children or young person 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 work 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 your organisation's policy. All staff are strongly advised to ensure that they understand the organisation 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 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. For example, a young person might prefer to text a report about bullying, rather than arrange a face to face discussion or may prefer that you arrange an appointment to see them by text rather than by letter.

Friendly verbal banter between adult and young person may not be inappropriate, but it might look very different if carried out via email or instant messaging e.g 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 a young person or an adult when in a professional setting.

Adults should be aware of, and comply with, the organisation policy on the use of text or instant messaging.

"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 Jan 2009).

Staff should never use their personal email address, home address or telephone line (fixed or mobile) to communicate with children, young people or clients.

In all situations a sudden or urgent communication must still be approved by their senior manager.

Personal online profiles or blogs should not identify the employer as any inappropriate information which could be considered to be bringing your employer/organisation into disrepute could lead to disciplinary action.

In all cases ensure that your relationships with young people are known, approved and recorded by your line manger or 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 have been 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's 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 organisation limit private online publishing?

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

A. One example of the risks of online publishing included a nurse 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; staff discussing a client in a shop queue might be overheard by a parent. However the technology enables messages to be recorded, edited maliciously, used out of context, republished 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-work conversation between friends to professional matters which is a breach of professional confidentiality.

Staff members should either be fully conversant with the security and privacy setting for the site in use or should avoid posting any information that could compromise their professional integrity.

Q10 How do I ensure safer online activity in a hospital classroom?

A. Most internet use in hospital classrooms is safe, purposeful and beneficial to patients 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 hospital system before use. You should direct patients to a specific website or a selection of pre-approved websites and avoid using search engines.

When working with older patients, 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 patients when planning online activities.

When encouraging patients to publish work online hospital wards should consider 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 and reassure the patient. To protect yourself you need to log and report the URL to a member of senior ward staff or the named nurse / child protection lead according to the organisation's 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 work computer to book holidays during lunch time or after work?
- How should I respond if I am subjected to cyberbullying by young people, colleagues or clients?
- How should I respond if I am subjected to cyberbullying by a child or young person?
- Can I respond to a comment about my team on the Friends Reunited site?
- May I use Bebo with year 8 pupils to discuss a history topic?
- Should I text a young person in the evening to remind him to of an appointment that has been arranged?
- How should I research Nazi sites to produce a lesson for sixth form pupils?
- Should children aged ten years of age use a search engine?

Links

1. Kent & Medway Safeguarding Children Procedures
   http://www.kenttrustweb.org.uk?kscbpolicy

2. Guidance for Safer Working Practice for Adults who work with Children and Young People (DCSF January 2009)
   http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00311/

3. Guidance for Kent Schools and Services on the Use of Photographic Images of Children
   http://www.kenttrustweb.org.uk/UserFiles/CW/File/Policy/Key_Policies/photographic_image_policy_0309.pdf

4. National Centre for Missing or Exploited Children
   www.cybertipline.com

5. Kent Schools e-Safety Policy and Guidance 2010
   www.kenttrustweb.org.uk?esafety

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:

Kent Safeguarding Children Board has their own Resources and Library page on e-Safety
www.kenttrustweb.org.uk/new_kscb/kscb_library_esafety.cfm

KENT SAFEGUARDING CHILDREN BOARD ©
Sessions House
Maidstone
Kent

01622 694659

www.kscb.org.uk