

SAFER PRACTICE WITH TECHNOLOGY - FREQUENTLY ASKED QUESTIONS



PROMOTING E-SAFETY IN NORTHUMBERLAND SCHOOLS

e-safety training
policy & procedures
countywide accreditation & support
network controls
incident reporting

WHAT'S IN THE PACK?

THIS DOCUMENT FORMS PART OF A PACK AIMED AT PROVIDING AN INTEGRATED APPROACH TO DEVELOPING SCHOOLS AS E-SAFE COMMUNITIES. OUR APPROACH HAS BEEN TO INTEGRATE THE RESOURCES, SUPPORT AND GUIDANCE AVAILABLE TO SCHOOLS INTO A SINGLE PACK OF MATERIALS PROVIDED WITH THIS DOCUMENT. THESE INCLUDE:

- Training materials for a variety of groups provided on cd-rom;
- Guidance and sample documents to help schools develop and implement policy and procedures also on cd-rom;
- Resources to help monitor and control network use and internet access, provided on the USB memory stick;
- Strong links with the Northumberland Safeguarding Children Board and the promotion of their materials and guidance, particularly the incident reporting flowchart;

And drawing this all together:

- A countywide accreditation scheme linked to the above resources and underpinned by support and guidance from the Local Authority e-learning and ICT support team.

The pack distributed to schools contains:

1. 'An integrated approach to developing schools as e-safe communities' which forms the core of the pack and three other documents;
2. This document - 'Safer practice with technology -Frequently Asked Questions';
3. 'The e-safety self assessment tool';
4. Guidance on 'Implementing network control and monitoring tools';
5. A USB data drive which contains the software for installing Policy Central Enterprise on school computers;
6. A cd-rom containing the training materials and additional resources such as exemplar policy documents and templates;
7. Information on registering your school for accreditation;
8. Information on training courses linked to the integrated approach, and covering e-safety and also network control software (PCE).



Support and guidance available to schools into a single pack of materials.

SAFER PRACTICE WITH TECHNOLOGY

Northumberland County Council is committed to helping children and young people and, adults working with them, to understand the risks of being online to the World Wide Web and take measures to protect themselves, whether from hackers, viruses, cyberbullies or online strangers that may want to harm them.

Protecting young people, and adults, properly means thinking beyond the traditional school/care environment. Where once the desktop computer was the only way to access the internet, now many mobile phones and game consoles offer broadband connections.

Our students, professional staff and carers may work online in settings, at work, at home or in an internet cafe. They may have personal devices not covered by network protection and therefore we need to ensure everyone understands the risks and acts accordingly. Safeguarding children and young people in both the real and virtual world is everyone's responsibility. The setting may well make use of technology such as Policy Central Enterprise, however any establishments relying solely on technological solutions could be placing themselves, and their pupils and staff, at risk.

Adults who work with children 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 and is largely based on those working in paid or unpaid capacities, in a school context.

However, the same principles can be applied to adults working as carers or in a caring profession, for example, foster parents, social workers etc. Many of us feel unsure or anxious in our approach to technology. Others are more confident but are unclear of the risks or the breadth of areas of concern. A rules approach cannot resolve all 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. It also provides examples of incidents that have occurred both locally and nationally, to give credibility to the need for awareness, and for individuals to take responsibility for their actions in this area.

The Council has been actively promoting e-safety through training courses, teaching materials, template documents and senior leadership meetings. This sustained focus on e-safety has been drawn together in the 'Promoting e-safety in Northumberland' documents and the 'e-safe Northumberland Schools' strategy.

Recently, a number of schools in the County were subject to an e Safety audit to compare how individual establishments were complying with the e-safety agenda and to determine whether additional training was necessary. From this, it was clear that many schools needed additional support and that further advice would be beneficial.



Protecting young people, and adults, properly means thinking beyond the traditional school/care environment.

This document seeks to provide answers to questions posed during the audit and explain some of the reasons why specific risks need to be addressed. Whilst this document focuses on controls that should be applied when working with technology, it is worth bearing in mind that it is our professional judgement and practice that will really make the difference between a situation being safe or not. If you do not feel confident in making that judgement, do not proceed with the activity and seek advice.

The local authority, schools and staff cannot 'police' the internet, nor guarantee to block all undesirable materials or risks to users, but what we can do, is to develop our own professional practices and understanding to ensure that children in our care are well protected and educated in the dangers and responsible use of the Internet and technology.

This document may provide some answers to your concerns and queries, more than likely, it will throw up further questions and generate greater debate in schools and settings. We need to have these debates if we are to develop our understanding of the risks and benefits of technology and inform our practice.

The e-learning & ICT support team and the Northumberland Safeguarding Children Board welcome feedback on this document and the other materials provided with the 'Promoting e-safety in Northumberland Schools' pack.

The author would like to thank Kent County Council for sharing literature, which is used in this document.

THIS DOCUMENT AIMS TO:

- Help adults reflect on their current use of technology.
- Assist adults to work safely and responsibly and to monitor and improve 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.



This document may provide some answers to your concerns and queries, more than likely, it will throw up further questions and generate greater debate in schools and settings.



FREQUENTLY ASKED QUESTIONS

- Q1** Should I use my mobile phone to take photographs of children or to communicate with children or parents?
- Q2** Should I continue to use my Social Networking site?
- Q3** Should I have children as friends on Instant Messaging services and/or Social Networking sites?
- 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 network use? As a leader, should I also be monitoring network activity?
- Q9** Can my workplace limit private online publishing?
- Q10** How do I ensure safer online activity in the primary classroom?

**Based on
“Guidance for
Safer Working
Practice for
Adults who work
with children and
Young People”
DCSF Nov 2007**



IF IN DOUBT

- Consult your policy documents for discussion with your designated person for e-safety and line manager.
- Consider how an action would look to a third party, such as a parent, governor and local newspaper.
- Only publish content that you would be happy to share with parents, pupils and your employer.
- Ultimately, if you have a concern, use the NSCB flowchart to help you decide how to proceed and visit <http://ngfl.northumberland.gov.uk/e-safety> for up to date guidance.

USING THIS DOCUMENT

- Provide copies when staff sign their establishment's Acceptable Use Policy.
- Organise a staff development session around these FAQs.
- Add this guidance to the staff induction pack and place in staff areas.
- Feed back to NSCB other issues so that we can all share our experiences and develop our understanding.

Feed back to NSCB other issues so that we can all share our experiences and develop our understanding.

Q1

SHOULD I USE MY MOBILE PHONE TO TAKE PHOTOGRAPHS OR VIDEO OF YOUNG PEOPLE, OR TO COMMUNICATE WITH YOUNG PEOPLE OR PARENTS?

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 workplace-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 work equipment there is at least a demonstration that the photography was consistent with organisation's policy. Please also refer to the NSCB guidance on the Use of Photographic Images of Children, a copy of which can be found at:

<http://ngfl.northumberland.gov.uk/e-safety> 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 work allocated laptop might make it difficult to retain control of how the picture is used and/or viewed by persons other than the member of staff. Memory cards, memory sticks and CD's should only provide a temporary storage medium and it is considered good practice to keep personal and professional storage media separate to prevent accidental or malicious disclosure of personal information. Once photographs are uploaded to the appropriate area of the organisation's network images should be erased immediately from their initial storage location.

The DCSF guidance 'Cyberbullying, Supporting School Staff' gives the following advice regarding mobile phones:

'Mobiles can be used very effectively to support learning, allowing learners to document project work, for example by using images, voice and text. However, most schools have also experienced problems with the disruptive use of mobiles and should have clear guidelines about acceptable use, developed in consultation with the whole-school community. Almost all schools have policies that prohibit the use of personal mobile phones during lessons.'

Guidelines should be enforced consistently by all school staff, and supported by the school leadership team.

School staff can confiscate a mobile phone as a disciplinary penalty, and have a legal defence in respect of this in the Education and Inspections Act 2006 (s 94). Staff cannot search the contents of a pupil's mobile phone without the consent of that pupil. Where a pupil refuses to allow the contents of his/her phone to be searched, the matter can be referred to the police who have more extensive search powers. If the pupil is suspected to have committed a criminal offence, it may be advisable to involve the police from the outset.

The safest approach is to avoid the use of personal equipment and to use a workplace-provided item



School employees should take good care of their mobile phones. They should secure their phones when not in use, using the phone's security code. If a phone goes missing or is suspected as being stolen, it should be reported to the police and mobile operator as soon as possible, using the phone's unique International Mobile Equipment Identity, or IMEI number. This can be found printed on the phone underneath the battery, or by typing *#06# on a handset.

Employees should be given clear guidance regarding the use of their personal mobile phone by their employer, regarding having access to pupils' numbers, storing pupils' numbers, and giving pupils access to their personal numbers.'

It is important to continue to celebrate achievements of pupils through the appropriate use of photography in communicating with parents and the community. As a basic rule, only work equipment, phones, cameras and computers should be used by pupils.

A recent e safety audit highlighted that some teaching staff are using their own mobile telephones to speak to students and their parents. This could be to provide feedback (positive and negative) and to try and progress delivery of course work which is due to be assessed in accordance with national deadlines. In using a personal telephone, the audit trail of the call cannot be guaranteed and the caller ID (the user's personal telephone number) could be disclosed. This could subsequently be abused and the staff member has effectively lost their privacy. It would also be more difficult to defend any allegation of inappropriate communications and is contrary to DCSF guidance on cyberbullying of staff.

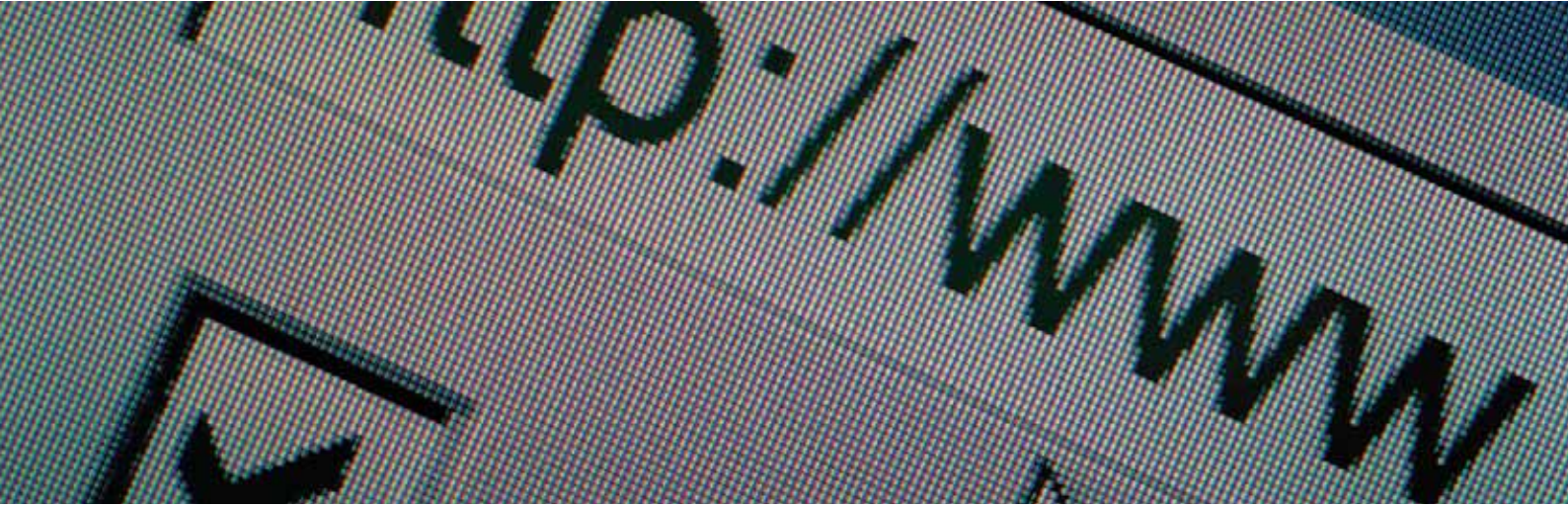
No, do not use your personal phone. Where possible workplace devices should be used to record images or communicate with pupils and parents. It is also recommended that use of work mobile telephones is monitored to ensure compliance with the organisation's policy and that an inventory of camera, telephones and other equipment is maintained.

Q2

SHOULD I CONTINUE TO USE MY SOCIAL NETWORKING SITE?

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. Take care that your Facebook friends are also aware that if they post photographs of you and tag them (name the people in the photograph) this too will

Employees should be given clear guidance regarding the use of their personal mobile phone by their employer,



be available for other people to see and copy unless their profile is adequately protected and you will have no opportunity to edit this material.

False social networking sites have been set up by pupils and adults with malicious information about staff. In one local school, a student sent abusive comments to a teacher, whose profile had not been adequately protected. More worryingly, another male pupil at the same school copied the thumbnail picture of the teacher and posted this onto a new profile he had created. The student then used this profile to communicate to other Facebook users, who would have thought that they were communicating with an adult. The teacher's integrity could also have been compromised if the profile had been used to display disparaging or inappropriate material, especially as he would have been unaware this was happening.

Consider also, the recent cases highlighted within the national news whereby staff working with young children have faced prosecution following inappropriate relationships with young people, a number of which started with communications on Facebook. Any such communication not conducted through formal work channels can be taken out of context and result in allegations of misconduct.

Some adults have been caught out by posting amusing remarks about their workplace 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).

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

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 workplace, even though many pupils disregard this legal requirement. For this reason, Northumberland County has taken steps to prevent access to social networking sites via the school network as there are a variety of other ways to communicate and share information with parents and pupils online e.g. NorTLE.

Yes, continue to use Social Networking Sites but bear in mind the DCSF guidance which states, 'Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it.'

Some adults have been caught out by posting amusing remarks about their workplace or colleagues, only to find them re-published elsewhere by "friends".



Q3

SHOULD I HAVE MY PUPILS AS FRIENDS ON INSTANT MESSAGING SERVICES?

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, however innocent they may think this is. 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 Nov 2007). School staff should also be aware of circular letter G52/09 ref SI/JD/JK/C47 dated 15th April 2009 and published via the schools courier ‘Use of Social Networking Sites by Adults who work with Children and Young People’. Please note that this does not just apply to teaching staff, this guidance is for anyone working in whatever capacity where they may be in contact with young people. This includes support staff such as lunchtime supervisors, cleaners etc. AUPs should clearly state this and all staff informed.

Consideration should be given as to how this type of communication might appear to a third party. Compared with a conversation in the workplace the use of new technology inevitably increases the potential for messages to be seen out of context or misinterpreted. Staff need an online environment which is under their control. The first requirement is that you know whom 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.

Also be aware that most mobile telephones have Social Networking and Instant Messaging software pre-installed, this further exacerbates the risk of staff using their own mobile telephone for any communication with young people and parents.

No, pupils should not be added as friends. Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Online communication provides excellent opportunities for collaborative work between groups of pupils. Monitoring or tuition, where appropriately arranged, could guide and enhance such activities. However, make sure staff understand what is appropriate.

Adults should not share any personal information with the child or young person, however innocent they may think this is.



Q4

WHAT IS MY RESPONSIBILITY FOR THE USE OF MY WORK LAPTOP AT HOME?

Internal audit has been required to investigate a number of alleged incidents regarding the misuse of laptop computers by staff working in Northumberland County Council. Whilst some of these have turned out to be innocent or accidental misuse there are other instances where use has been deemed to be inappropriate leading to disciplinary action.

So what can go wrong?

When using the laptop computer to access the Internet at work, there are suitable software controls in place to minimise access to inappropriate material e.g. PCE software. However, when accessing the Internet at home, no such controls may exist. 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 that may be stored on the hard drive has not been accessed. Alternatively the user may not know that their friend has saved personal information onto the hard drive and this may be disclosed causing embarrassment or harm.

Adults vary enormously in their judgements as to what is appropriate, funny, acceptable and offensive, whether this is in the form of web sites, images, text or video clips. Some adults may feel that access via a work laptop to adult material outside work 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 as images are stored on the hard drive 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, think about whom would be culpable in certain situations.

If the organisation's policy sanctions personal use of the work laptop at home, Policy Central Enterprise should be installed. Adults should refer to their organisation's policy on the personal use of work laptops, which unfortunately varies between settings and between local authorities. Increasingly the use of a work computer for non-professional use is being explicitly banned. Any school or other organisation which allows personal use should implement appropriate controls to regularly review and monitor such use for compliance with Acceptable Use Policies. Further advice on how this can be achieved is available from ITSecurity@northumberland.gov.uk

If the organisation's policy sanctions personal use of the work laptop at home, Policy Central Enterprise should be installed.



In addition, users should be advised that any material produced on behalf of the workplace should be saved on the work network. One school within the County had all of their policies saved on one particular laptop. When the member of staff left for alternative employment, they wiped the hard drive and all of the policy documents were lost. If you need it, save it on the network where it should be regularly backed up for contingency purposes.

“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 work laptop allocated to their use.

Q5

WHAT IS INAPPROPRIATE MATERIAL?

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 might 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 are 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 cyber bullying 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. There have already been two instances, which have been subject to audit investigation within the County where disparaging remarks have been made about individuals and County Council organisations on Facebook. AUPs should include guidance on use of Social Networking Sites.

Inappropriate is a term that can mean different things to different people.



These are real examples of inappropriate misuse within the County:

- Posting offensive or insulting comments about the workplace on Facebook.
- Accessing adult pornography, dating websites etc on workplace computers during and outside working hours.
- Using work telephones to access adult material and chat lines.
- Using work equipment to store indecent images of adults and children.
- Using workplace digital cameras to take inappropriate images of minors.
- 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.

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.

Q6

HOW SHOULD I STORE PERSONAL DATA SAFELY?

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 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. The County Council has a policy on the protection of personal information, which can be found on www.northumberland.gov.uk

Your setting should have a policy and staff are strongly advised to ensure that they understand their individual responsibilities regarding data protection as legal action could be taken against the individual rather than the organisation. To lose control of personal data while not complying with the organisation's policy would be difficult to defend.

Q7

HOW CAN I USE ICT APPROPRIATELY TO COMMUNICATE WITH YOUNG PEOPLE?

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. Nor should emails be signed off using personal or intimate language.

There are a variety of other ways to communicate and share information with parents and pupils online e.g. NorTLE

Adults should be aware of, and comply with, the setting/authority policy on the use of text or internet messaging systems. '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). Organisations should specifically prohibit staff using their personal email addresses or telephone 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.



Friendly verbal banter between adult and pupil may not be inappropriate, but it might look very different if carried out via email or MSN



Q8

AS A TECHNICIAN, HOW CAN I SAFELY MONITOR NETWORK USE?

Filtering or recording network usage will only be effective if monitored carefully to notice and report inappropriate access or usage. This responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity. Organisations should not assume that it is the sole responsibility of the technical staff to monitor the network.

The LA has provided Policy Central Enterprise (PCE) to all schools and this should be managed and monitored by someone on the Senior Management team, ideally the person with responsibility for e-safety. Technical staff and other colleagues in the monitoring role may well assist this person.

Northumberland County Council is part of a collaborative agreement between local authorities using DurhamNet to filter access to the Internet in schools. Likewise the County Council use McAfee to filter access to the World Wide Web. These software packages are designed to restrict access to inappropriate web material, banning categories such as adult material, gaming etc. 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; they have access to DurhamNet and can ensure inappropriate sites are promptly banned.

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 organisation's designated child protection co-ordinator and pastoral staff. A technician might, with the best of intent, check sites that a user

technical staff should not be expected to make judgements as to what is inappropriate material or behaviour, without support and supervision.



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 workplace procedure, but staff should ensure that they receive a specific, written request to perform this work.

Use tools such as Policy Central Enterprise and when an e-safety incident occurs, 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 e-safety flowchart will guide the organisation's, carer's and professional's response to an incident of concern.

Q9

CAN MY WORKPLACE LIMIT PRIVATE ONLINE PUBLISHING?

Care needs to be taken to ensure that staff behave professionally in their use of internet services when online.

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, 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 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.

The DCSF guidance states, 'While employees are private individuals, they also have professional reputations and careers to maintain...'

Care needs to be taken to ensure that staff behave professionally in their use of internet services when online.



Q10

HOW DO I ENSURE SAFER ONLINE ACTIVITY IN THE PRIMARY CLASSROOM?

Most Internet use in the workplace 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 workplace 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. 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 establishments e-Safety policy. Avoid printing or capturing any material.

As previously highlighted, the Local Authority has provided PCE to all schools as part of the strategy to promote e-safety in Northumberland. This should be installed on all desktops and laptops as it provides a range of tools, including those for filtering and blocking.

Most Internet use in the workplace is safe, purposeful and beneficial to pupils and staff. However, there is always an element of risk.

FURTHER QUESTIONS FOR DISCUSSION

These might be used to initiate further staff discussion:

- Can I use a workplace computer to book holidays etc during lunchtime or after work?
- 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 workplace 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?
- As a student teacher/supply teacher/visitor/contractor, does the AUP apply to me?
- As a student teacher/supply teacher, are there particular risks that I should be aware of?
- I work in the school but am not directly employed by them, what's my responsibility?

AND FINALLY...

- **Keep your password safe and secure. This is becoming more important as staff are given access to pupil demographic data for registration purposes. Log out of the computer system when you are not using it to ensure your user profile is not abused. A teacher left a laptop unattended and logged into the school network. A pupil uploaded inappropriate images (via the laptop) to the shared area of the school network via her mobile telephone. What if that had been an unauthorised visitor who was able to access personal information about a vulnerable child?**
- **Be vigilant about the information displayed on notice boards etc that may be viewed by members of the public when using school facilities out of hours or during parental meetings and student assemblies. Any personal identifiable information, whether this is regarding students, staff parents etc should be removed from sight and stored securely with access restricted to only those persons needing to see this to support their work. Information about student medicines should be stored inside the medicine cabinet, not stuck to the outer door. Information regarding vulnerable students should only be stored in the staff room if that area is secure and access is restricted to staff only.**
- **Do you know who is inside your workplace? Whilst first schools have physical access restriction, preventing unauthorised access to the premises, some of the larger middle and high schools have multiple uncontrolled entrances. If this is unavoidable, ensure that all staff wear badges clearly identifying them as members of the school personnel. Ensure visitor access is recorded, visitors are badged and accompanied at all times where practicable. This will allow easier identification of people who may have no legitimate business on the school premises.**
- **Further information is always available from the NGfL website:
<http://ngfl.northumberland.gov.uk/e-safety>**



Log out of the computer system when you are not using it to ensure your user profile is not abused

CONTACTS AND FURTHER INFORMATION

LOCAL

Russell Pilling - Head of safeguarding
russell.pilling@northumberland.gov.uk

Janet Ingham - Business manager for Northumberland Safeguarding Children's Board
Janet.ingham@northumberland.gov.uk

John Devlin - ICT Consultant
john.devlin@northumberland.gov.uk

Richard Taylor - ICT & e-learning Adviser
richard.taylor@northumberland.gov.uk

Chris Heane - Computer Services Network and Security manager
Chris.heane@northumberland.gov.uk

Andrea Carmichael - Local Authority Designated Officer
Andrea.carmichael@northumberland.gov.uk

Northumbria Police
www.northumbria.police.uk

NATIONAL

Child Exploitation and Online Protection
www.ceop.gov.uk

Childnet International
www.chlidnet.com

Becta
www.becta.org.uk



An integrated approach to developing schools as e-safe communities.

02

PROMOTING E-SAFETY IN NORTHUMBERLAND SCHOOLS

Learning and Development 0-19 Service
Learning, Skills and Family Support
People Directorate
Northumberland County Council
County Hall
Morpeth
NE61 2EF

Telephone: 01670 533000