Staff Guidance on Staying safe with use of New Technologies

Acknowledgement

This document has been adapted for use within Wakefield Schools from the original document 'Safer Practice with Technology for Adults working in schools' produced by Kent Public Service Network www.kenttrustweb.org.uk?esafety

Questions

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

Photography by pupils and staff are encouraged for curriculum use and are an essential part of any school visit, but there are potential dangers.

The safest approach is to avoid the use of personal equipment and to use a school-provided item. A 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 show that this was not the case. With school equipment there is at least a demonstration that the photography was consistent with school policy. It is important that the Guidance on the Use of Photographic Images of Children is referred to www.gowild.org.uk/dataprotection

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 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?

Social networking is a 'normal' part of life for most young people and many adults. However, adults working with children and young people should review and reflect upon their use of social network sites as they take on professional responsibilities. This includes checking back on redundant sites that may still be active.

Strong passwords[1] should be used and security settings should be applied so that **you** control all access to your profile. Once Information is published, (photographs, blog posts etc) you lose control of them and they may be manipulated without your consent, used out of context, inappropriately or distributed further.

[1] Use of 7 characters or more including at least 1 capital letter and a number.

What might seem an amusing remark posted about your school or colleagues, may end up re-published elsewhere by “friends”. False social networking sites have been set up by pupils and staff with malicious information. Currently few public social networking sites authenticate their members and use automated registration systems which provide limited if any checks. Some instant messaging applications such as MSN have a facility to keep a log of conversations. “Don’t publish or say anything online that you would not write down and display on the staff room notice board !

Q3 Is it alright to have pupils/students as friends on my social network site or instant messaging service?

Communication between adults and children/young people, by whatever method, should take place within clear and explicit professional boundaries.

Staff 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. Therefore, requests to be a ‘friend’ on any social network site should be ignored.

“Adults should ensure that all communications are transparent and open to scrutiny.” (DCSF Nov 2007) For example ensuring all communications by all parties, use official school email or Learning Platform systems and is purely for teaching and learning purposes.

Consideration should be given as to how communications 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.

Staff must use an online environment which is under the school’s or Local Authority’s control. The first requirement is that you know who you are talking to; users must be authenticated. A School/Local Authority/RBC provided communication and collaboration area will have a range of security features set within a policy framework.

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

Access to wider sites by family members, for instance accessing gaming site or less well known shopping sites will increase the risk of virus attack, unwanted adware 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’ views vary enormously in their judgements as to what is appropriate!

The use of a school laptop to view adult material outside school hours and at home is inappropriate and may be illegal. The schools acceptable use policy

should state whether the use of school equipment for appropriate personal use is acceptable (see Q5 for guidance of appropriate use) . There are cases where inappropriate access has led to dismissal.

School staff 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. Increasingly the use of a school computer for non-professional use is being explicitly banned by schools.

School staff should therefore ensure that they have absolute control of a school laptop allocated to their use.

Q5 What is inappropriate material/use?

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 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 bullying by mobile phone, social networking sites etc (cyberbullying). 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.

Some possible examples:

- Posting offensive or insulting comments about the school on Facebook.
- Accessing adult pornography on school computers during break or on school laptop at home
- Making derogatory comments about pupils or colleagues on social networking sites.

- Contacting pupils through personal email or social networking sites is inappropriate and should not occur under any circumstances, unless authorised under special circumstances by the Headfteacher.

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.

Family Services and e-services are working on providing practical guidance for schools in keeping data secure. Guidance on Information security can be found at www.gowild.org.uk/esafety

All personal information must be kept secure. Making such storage secure may include password protection, encryption of data and locking the computer when not in use. Please refer to the guidance document on information security referred to above and your ICT support service. The mislaying a memory sticks are all too common. Even the use of encrypted memory sticks should only be seen as temporary storage of personal data, and only if necessary and ensuring files are deleted after use. The EdIT centre can advise on suitable encrypted memory sticks that have been tested by e-services.
The safest long-term storage location may be the school network. ”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 the school policy regarding data protection. All schools should have a data protection policy.

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

Using ICT to communicate with pupils/young people should be done through the school’s Learning Platform in an appropriate online open shared environment such as a class forum. Friendly verbal banter between adult and pupil may not be inappropriate, but it might look very different if carried out via email and might lead to difficulties if misinterpreted, forwarded or used out of context. See Q3

On no account should staff use their personal email addresses or phone numbers to communicate with young people.

Q8 As a technician, how can I safely monitor school network use?

Filtering is provided by YHGFL for schools in Wakefield and this filtering is accredited by Becta. If the school has monitoring software in place for recording network activity, this can only be effective if monitored carefully to

notice and report inappropriate access or usage. This is a senior responsibility and will require oversight and allocated time of a senior member of staff. Leaving this role solely to a technician in school is not adequate and the responsibility can become onerous if a pupil or staff member is apparently implicated in inappropriate or illegal activity. Careful consideration about the use of monitoring software should be given and all staff and pupils informed if applied to the network. Educating pupils/young people about appropriate online behaviour in school and outside school be an integral part of teaching and learning programmes.

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.

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.

Questions for Discussion

- Can I use a school computer to book holidays or check my bank account during lunch time or after school?
- Can I search for my pupils' entries on Facebook to check what they are sharing publically?
- 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 Facebook 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?
- Is it safe for my year four pupils use google image search?

Links to esafety and information security

www.gowild.org.uk/esafety

www.gowild.org.uk/datprotection

Wakefield District Safeguarding Board
http://www.wakefield.gov.uk/HealthAndSocialCare/ChildrenAndYoungPeople/SafeguardChildren/default.htm