Department of Education

LET'S FACE IT ©

Staying safe with information communication technologies (for school based staff)

First printed 2010

Prevention and Education Team
Standards and Integrity Directorate

Current as at 15.07.2010

Learning Outcomes

By the end of this presentation, participants should be aware of:

- The risk areas in relation to social media and ways to minimise these risks.
- The Department's *Information and Communication Technologies* policy; in particular, how it relates to confidentiality and the use of Departmental computers and online services.
- The Department's *Duty of Care Policy* including the responsible use of technology and the supervision of students using the internet and media texts.
- The Department's *Child Protection Policy* regarding social interaction with students via social networking sites.
- The Department's *Students Online Policy* and the requirement for schools to have appropriate procedures and policies in place to manage the use of online services by students.
- Those sections of the *Criminal Code* dealing with unauthorised access to restricted material.

This presentation covers the following risk areas:

- Web socialising/social media
- Unauthorised disclosure of confidential information
- Inappropriate use of DoE computers and online services
- Duty of care and cyber safety
- Breach of copyright

What is social media?

Social media is an umbrella term that defines the various activities that integrate technology, social interaction, and the construction of words, pictures, videos and audio. This interaction, and the manner in which information is presented, depends on the varied perspectives and "building" of shared meaning, as people share their stories, and understandings

(Source: Wikipedia)

Relevant Information technologies and social media include Facebook, Twitter, email, SMS, YouTube, and transmission of images via mobile phone/computer. All of these applications pose privacy and security challenges.

Staff need to be aware of relevant policies and codes of conduct that relate to the use of new technologies. If you are unsure, get advice or you might be more of a "twitter" than you think! Test your understanding by completing the True/False activity below. Write T or F in the margin.

1. It is acceptable to *bluetooth* a video of a school fight to the mobile of a teaching colleague in another school to illustrate how tough it is to work in your school.

2. You are permitted to check your personal email on the work computer in your office during your lunch break.

3. During the Easter break, you are concerned about a student in your class who seemed a bit down on the last day so you decide to send them a cheery email via hotmail. This is considered acceptable contact.

4. Teachers are not permitted to invite students with whom they have a good relationship to join their *Face Book* pages.

5. It is acceptable to download pornography on your *Notebook for Teachers* laptop computer as long as it is outside of school hours and the school premises, and, is not child pornography.

6. It is permissible to share your teaching experiences with work colleagues and friends on T*witter*.

7. A teacher has the right to confiscate a student's mobile phone if the student is using the phone inappropriately.

Communication Technologies/Social Media

Engaging with new technologies presents a number of risks for school based staff. Of particular concern is the ease with which professional distance and appropriate staff-student conduct boundaries can be breached. A number of Department policies and both State and Federal legislation regulate the use of these technologies within a school setting and in private use. All employees need to understand these regulations so that their use of these technologies is effective and responsible. As with many ethical dilemmas that teachers face, the issue of interactions with new communication technologies or social media are complex. For many people, web-based communications are an integral aspect of their social and professional lives. They are also recognised as valuable learning tools. Staff are increasingly required to:

- use new technologies as part of their teaching, learning and assessment programs. This may include the creation of applications such as web pages and blogs;
- communicate with parents and students regarding homework and student progress via email;
- encourage these forms of communications as legitimate texts to study in learning areas, for example, English and Media Studies.

Staff must ensure that these legitimate applications do not place themselves or their students at risk.

Identifying Risks

Many of these applications engender a false sense of *anonymity* – a feeling that, when using these applications, our identity is secret and recipients don't know who we are. Web socialising in particular encourages high levels of intimacy. We may do and say things that we would never do or say normally when face to face with someone. This overconfidence may lead to a blurring of professional boundaries that in turn could result in:

- allegations of teacher misconduct, specifically, inappropriate contact with students or inappropriate conduct outside of school hours;
- the unauthorised sharing of confidential Information.

Where staff fail to comply with the relevant DoE policies, there could be complaints alleging staff misuse of DoE online services. Perhaps, more significantly, there may be inadequate supervision of students leading to student misuse of DoE online services and/or cyber bullying.

Conduct outside of school/web socialising

School based staff have both a public face and a private identity. Whilst you are entitled to a private life, you need to be mindful of behaviour in your private life that could impact on your public role and the reputation of the Department. The impact of new technologies, particularly web based 'socialising', means that aspects of a staff member's private life can become very public and could result in that staff member being vulnerable to allegations of misconduct.

In the same way that a staff member may take precautions when engaging in social activities in the broader community, especially where there is a close proximity to their school, they need to be aware of how web based 'socialising' and the applications of new technologies may impact on their role in a school setting. Employees can be found guilty of misconduct even outside school hours and off

school premises if a relevant connection can be made between that behaviour and their capacity to effectively carry out their duties.

Staff need to be aware that web socialising with students could easily be classified as 'conduct open to misinterpretation' given that it mirrors the grooming behaviour of paedophiles. Staff are **not** permitted to engage in social interaction with students via social networking sites unless there is an educationally valid context.

To minimise the risk of misconduct allegations, staff should not share personal email addresses, Face Book identities or online chat rooms with students.

Staff should not have special arrangements with selected students for web contact outside school hours, which involve servers other than the DoE server. Further, mobile phone contact with students in or outside school hours should only be made by staff using authorised school mobile phones.

Staff also need to be careful with the material that they put on the Internet on pages such as *Face Book*. Inappropriate information may be accessed by students or others who may consider the material fair game for access or for forwarding on to friends if the pages are not marked as private. This could result in allegations of misconduct. Web conversations with friends and colleagues about students and/or school business would also be considered highly inappropriate and a breach of the Department's *Code of Conduct*.

The guidelines for physical contact with students are also relevant to web contact. In particular:

- The greatest scope for misinterpreting staff behaviour is provided where a staff member interacts one-to-one with his/her students outside of the classroom;
- Contact with students inside and outside of the classroom is best done with public visibility and within earshot of others, preferably other staff members.

Stop-Think-Act

In the *Accountable and Ethical Decision Making* Training Course, the need to "Stop and Think" before deciding to act is emphasised. The *Stop-Think-Act* approach involves asking some searching questions about your proposed behaviour:

- Am I doing the right thing?
- How would others judge my actions?
- How could my actions impact on others?
- Should I discuss this with someone else?

Always consider context, purpose and impact

When considering the use of communication technologies with students, staff need to consider the **context, purpose** and potential **impact** of the use. As a guideline, staff should engage in Internet communications with students only:

1. In the **context** of their teaching and learning program and according to the school's policies for Internet use and communication with students and parents.

2. When the interaction has a clear **purpose** that relates to teaching and learning not socialising.

3. When the educational benefits of using the internet communication clearly outweighs the risk of students making inappropriate use of the opportunity thereby creating an adverse **impact**.

Use of Departmental Computers and Online Access

The Department has a comprehensive policy covering the appropriate use of its equipment and online services. ***All employees have a responsibility to read this policy*****.** The following extract outlines the scope of the policy:

*"*Staff *and contractors of the Department of Education must only use telecommunication resources, including computer hardware, Internet, intranet, electronic mail, faxes, telephones (fixed and mobile), for purposes that are legal, ethical and consistent with the aims, values and ethos of the Department. Staff must not deliberately access, download, store or send materials of a pornographic, racist, sexist, inflammatory, hateful, obscene or abusive nature".*

There are very strict rules governing the use of Department equipment and online services especially concerning the access of inappropriate material whether or not this access occurs on a school site. 'Inappropriate material' includes:

- Child pornography
- Objectionable material
- Restricted material

These are also offences under the *Criminal Code* (See *Relevant Legislation and Policies*).

Conditions of Use

In the *Conditions of Use* for the Department's computer equipment, staff accept that their use may be monitored. Staff are alerted to this each time they log on. It is also essential that staff protect the security of their password to prevent others from misusing their computer. Computers need to be locked when left unattended even for a few minutes.

A number of texts including websites, computer games and film that are not restricted in the public domain are restricted or prohibited in a school setting.

Staff are advised to check the ratings and content descriptions of such material very carefully before use. Staff have a clear *duty of care* to ensure that students do not access inappropriate material. Appropriate permissions need to be sought if material that may be considered sensitive is going to be viewed.

The personal use of telecommunication resources is permitted provided that use is not for commercial gain or in any way counter productive to the business of the Department. Employees need to use the "reasonableness test" in determining whether or not their personal use of these resources is appropriate.

Breaching Confidentiality of Information

Computers and access to online information pose a number of risks to the confidentiality of personal and/or sensitive information. Department employees must take care to safeguard data and ensure that they do not disclose data without authorisation. A *risk management* strategy might include:

- The safe storage of devices such as USB keys which may contain school data;
- Maintaining the confidentiality of user identification and/or passwords;
- Using extreme caution when transmitting media files via applications such as *Bluetooth*
- Being aware of the potential for misuse of Department data/information in emails or in web based discussions.

The misuse of computers and information is also covered by the *Criminal Code* (See *Relevant Legislation and Policies*).

Under criminal law, the Department's computer system would be classified as a "restricted-access computer system". There are prescribed penalties for unlawful use. All security or potential security breaches must be reported.

Emails and Confidentiality

Departmental policy has very detailed guidelines for the use of emails. Be aware that emails can be saved indefinitely on the receiving computer and can be retrieved once deleted. Once an email has been sent the sender has no control over the distribution of the email. Password protection and security labels are recommended in order to maximise security. Schools are advised to use disclaimers to limit liability in the event that staff or students use of emails is inappropriate.

It is important to consider whether or not an email is an appropriate means of communicating confidential information.

Some of the pitfalls of this form of communication are:

- High risk of exposure if inappropriate material is included;
- Recipients misunderstanding the tone and therefore the message;
- Interruption to work flow;
- People expecting an immediate response to challenging and/or complex issues;
- Important communications may be lost;
- Temptation to overuse because it seems a quicker method of communicating. However, other methods of communication such as a face-to-face meeting might be more effective.

Emails pose many challenges in terms of time management, effective communication and accountability. An email received in the course of your duty is considered a public record. As such, emails are subject to the Department's *Record Management Policy.* Schools are encouraged to ensure that they have clear guidelines for the use and management of email communication, including whether or not staff will communicate directly with parents and students via email.

Duty of Care and Cybersafety

Teachers have a *duty of care* to their students. A *duty of care* is the duty imposed by law to take care to minimise the risk of harm to another. In schools, this duty is to take such measures as are reasonable in all the circumstances to protect students from risks of harm that reasonably ought to be foreseen. The Department's *Duty of*

Care policy is relevant to the supervision of students engaging with technologies within the context of the classroom. Teachers have a responsibility to model and monitor the correct use of these technologies. In addition, teachers utilising these technologies in the classroom should be explicitly teaching students about identifying and minimising risks.

Risks fall into three main categories:

- Contact risks
- Content risks
- Confidentiality risks

When designing activities for the use of these applications in the classroom, teachers need to consider the likely **impact** and assess the potential risks of inappropriate use. Students need to be protected from exposure to inappropriate online material or activities, to be aware of the risks associated with some online activities, and to adopt protective online behaviour. Schools need to have comprehensive online use policies for students in place. See the *Students Online Policy* for assistance in developing appropriate policies and procedures.

A particular risk for students is *cyber bullying*. *Cyber bullying* occurs when students use mobile phones and/or the internet to communicate messages designed to bully another. Increasingly this involves the distribution of photos/images designed to ridicule the victim. There is considerable evidence regarding the impact of *cyber bullying*. In recent months there has also been significant attention to the side effects of *cyber bullying* which includes increased risks of depression and suicide. Whilst much of this bullying occurs outside of school, it can also occur in school. Teachers have a clear duty of care to protect students at school from *cyber bullying*. Adequate

supervision is an essential aspect of this. Appropriate use policies for devices such as mobile phones and cameras must also be in place.

Cyber Safety Resources

There are a number of resources available for teachers wanting assistance with teaching about cyber safety. The *Australian Communications and Media Authority* (ACMA) have a comprehensive approach to cyber safety education that targets teachers, children and parents. Schools are encouraged to work in partnership with parents to be proactive in dealing with *cyber bullying*. Whilst most of this bullying occurs outside of school, it may be directly related to events such as playground fights that occur during the school day on school premises. There are also a range of useful sites that provide strategies for parents and teachers including:

Childnet www.childnet.com,
NetAlert www.netalert.gov.au,
Netsafe www.netsafe.com.au,
Cyber safety net cybersafetynet.com/index.html
Cybersmart kids www.cybersmartkids.com.au,
Isafe www.isafe.org

Breach of Copyright

Another web risk area is the breaching of copyright. Departmental employees need to be aware of copyright issues as they relate to web-based material. The ease of copying and redistributing digital material makes this a high risk area for staff and students. It is often assumed that anything on the web is free to copy. **This is not so!** Whilst web browsing and some copying is allowable for the purposes of research and study (equivalent to the 10% allowed for books), copying and redistributing as attachments in emails or in some other publication is likely to be a breach of copyright. Teaching staff have a responsibility to educate students about copyright law.

It is important to note that in Australia, copyright protection does not require a copyright notice or any form of registration.

Schools have to be particularly careful in the creation of web sites. Often materials such as pictures, music, text, video clips and software are copyright. Key questions to ask when using copyright material:

1. Do you own the copyright?
2. Is the material in the public domain?
3. Does a defence or exception apply?
4. Is the amount insubstantial?
5. Do you have permission or a licence?

The answer to at least one of the above questions needs to be "**Yes".**

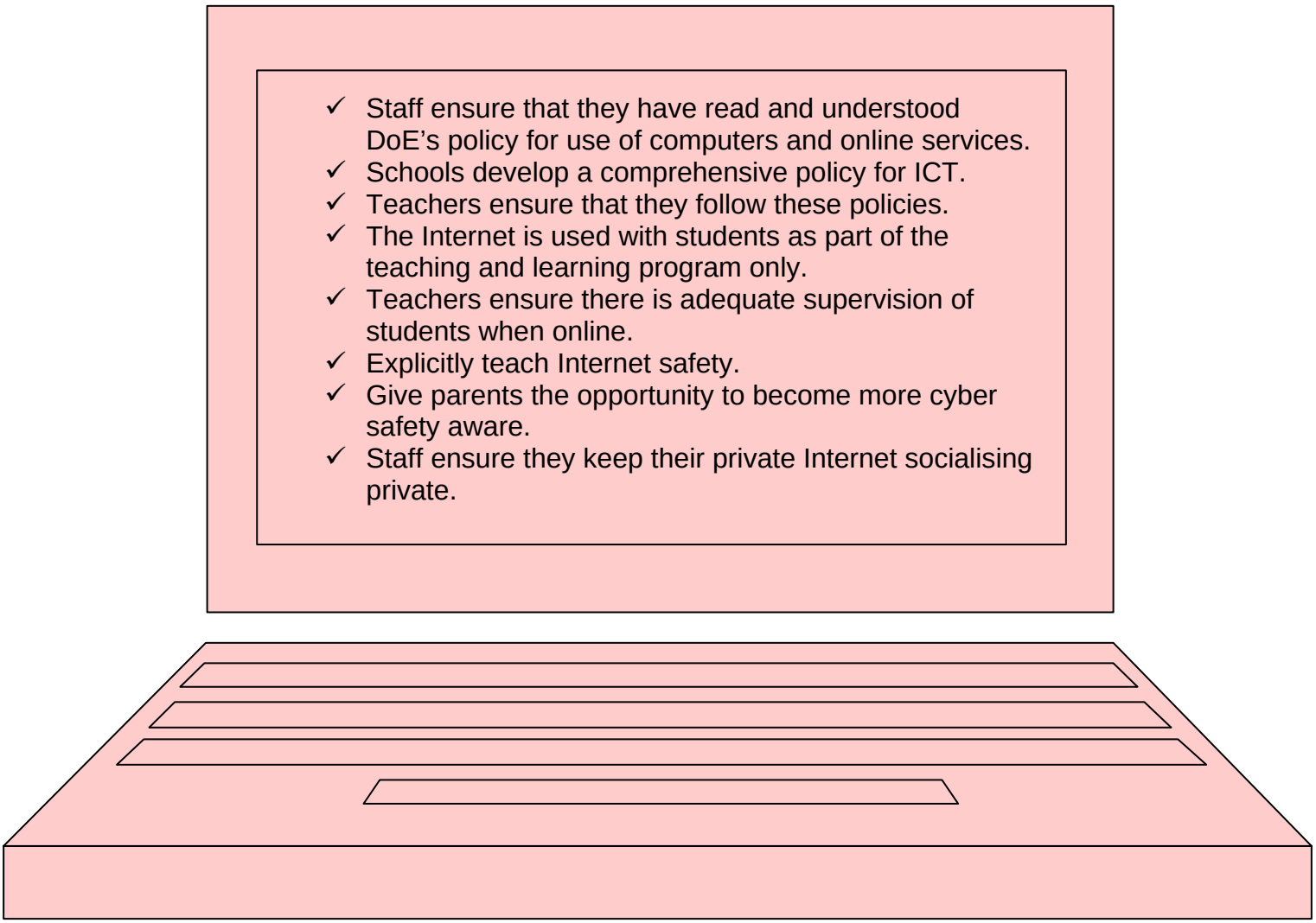
Schools need to protect unauthorised access to websites or databases through the use of firewalls and passwords. Detailed information concerning copyright including the creation of web pages, use of trademarks, and samples of disclaimers can be found in the Department's *Educational Institutions - Legal Aspects of Internet Compliance* policy.

Safety Toolkit for ICT Use

It is recommended that all employees make themselves aware of the relevant policies and legislation, which relate to the use of communication technologies and social media. Teachers in particular need to be very mindful of any information including personal profiles that they post on the Internet. Educators also have a responsibility to model and teach appropriate use of these new technologies.

Teachers who require assistance or support with the use of ICT in the curriculum including the creation of applications such as *blogs* should contact the Department's Online Curriculum Services at Central Office.

The following proactive strategies are recommended to minimise the risks associated with these new technologies:



Case Scenario

PART 1

Melanie is an art teacher who is highly regarded by her Year 12 class. At the end of the year when the students leave, she urges them to keep in contact and let her know how they get on. She receives an invitation to join the *Face Book* of one of the students in the class. Melanie considers the fact that this student has finished school makes this acceptable and is happy to accept the invitation. From time to time, she receives messages from the student and a number of other invitations from members of the graduating class. Frequently, their pages feature photos of their weekend parties. Occasionally, Melanie is a little concerned about some of the images and the discussions students have on the page but concludes that, since they are practically adults and she is no longer their teacher, it will be OK to continue on the Face Book site.

Questions for discussion:

1. ***What aspects of appropriate "teacher-student relationships" are relevant to events in Part 1?***
2. ***Is Melanie right to conclude that, as long as a student is graduating, she can continue contact through social media with that student without compromising her position as a teacher?***

PART 2

In class one day, Josh, a rather reluctant Year 10 art student who is heavily into work avoidance interrupts the class with the comment, "Jeez, you looked pretty pissed in that photo on your *Face Book* page Miss!" It soon becomes apparent that a number of students have accessed Melanie's *Face Book* page via ex-students. The students are keen to discuss the content of her page and compliment Melanie on some of the photos she has uploaded. The conversation gets out of hand quite quickly with students soon quizzing Melanie about her sex life and drug and alcohol consumption. Melanie makes the comment that she has also seen photos of some of their parties

and that her photos are in fact very ‘tame’. Melanie has a bit of a laugh with them and then directs the students back to their art projects. She congratulates herself on the excellent rapport she has with her students.

Questions for discussion:

3. ***What aspect of an appropriate “teacher-student relationship” has been undermined in Part 2?***
4. ***Has Melanie done anything improper?***
5. ***Is this classroom behaviour consistent with Departmental policies?***

PART 3

In the staff room at morning tea Melanie shares this experience with her colleague, Lisa. She is surprised to find Lisa is very disapproving of the *Face Book* contact with the ex-students. She advises Melanie to inform their Head of Learning Area about the conversation that took place in the class and take immediate steps to mark her page as *private*. Melanie thinks Lisa is overreacting and tells her that the students will lose interest quickly enough.

Questions for discussion:

6. ***What obligations under Departmental policies does Lisa have?***
7. ***Does Lisa have any professional responsibilities in this matter as a colleague of Melanie?***
8. ***What might the consequences of Melanie’s decision be?***

NOTES

Relevant Legislation and Policies

Commonwealth of Australia Law:

- Privacy Act 1988
- Telecommunications Act 1997
- Crimes Act 1914

Western Australian Law:

- Classification (Publications, Films and Computer Games) Enforcement Act 1996
- Corruption and Crime Commission Act 2003
- The Criminal Code
- School Education Act 1999

Western Australian Public Sector Codes:

- Code of Ethics

Department of Education Policies:

- *Duty of Care for Students*
- *Educational Institutions – Legal Aspects of Internet Compliance*

- *ICT Security Procedures: 1.2 Password and User I.D.*
- *Information Privacy and Security*
- *Information and Communications Security*
- *Staff Conduct*
- *Telecommunications*
- *Child Protection Policy*
- *Students Online Policy*

Western Australian College of Teaching:

- *Western Australian Professional Standards for Teaching (Version 3, 2009): Standard 8 - Professional Responsibilities*

Thank you for attending our presentation "Let's Face It". If you require further information about the issues covered in this presentation or have any queries, check out the references given first. Then, if necessary, contact the Standards and Integrity Directorate at DoE on 1800 655 985, or, the Principal Consultant Prevention and Education on 9264 4934, or, e-mail clem.wright@det.wa.edu.au