

Web 2.0 guidance for teachers

This guidance has been initiated by the PPTA ICT Taskforce as assistance for teachers in the use of Web 2.0 tools. The document is in two parts; it aims to provide brief and general guidance for teachers' use of Web 2.0 tools with classes, and provides some guidance for teachers' personal and professional safety using Web 2.0 tools.

Web 2.0 is the phrase coined to indicate the second generation of Internet tools. These tools include wikis, blogs and social networking sites.

Web 2.0 tools can provide useful and powerful teaching and learning opportunities for teachers and students who use them. However the insecure nature of the Internet environment can mean there is an element of risk for both teachers and students.

Guidelines on the use of Web 2.0 tools with classes

1. Where possible use of Web 2.0 tools should occur from within the school's Learning Management System (LMS)
2. Have a sound reason for using the tools - You may be challenged by the school community at some point, probably from a standpoint of 'is this appropriate?' The use of Web 2.0 tools should be based on sound educational reasoning, so it can be demonstrated that the benefits outweigh the risks.
3. Ensure you are competent. Teachers using and administering Web 2.0 tools need to be confident about doing this, and competent enough to respond appropriately in the first instance to incidents. They also need to be confident enough to answer questions from parents should they arise.
4. Review both staff and student use agreements and policies. Do this before you start to use the tools with your class. It should act as a reminder about both your and your students' obligations and responsibilities. You might also want to check beforehand that posting to the Internet is permitted.

5. When using tools choose sites for the entire school and look for ones that:
 - **Are designed for education.** This is more likely to align with your school aims and will have an education focus. The facility may already exist in your school learning management software.
 - **Are recommended by other teachers.** Don't let your school be a guinea pig for a site trying to cash in on the latest thing in education.
 - **Have an upfront usage policy.** This should be clear, easy to find, and contain guidance on appropriate use of the site. Look for a procedure for reporting inappropriate use also.
 - **Are easy to learn.** Choose a simple site that minimises opportunities to make mistakes.
 - **Allow posts and comments to be reviewed by teachers** before they are published to the site. Don't rely on site based moderators or filters to ensure postings are appropriate. These are too easily circumvented. Like it or not, the quality of the material posted reflects directly on your school and your teaching.
 - **Use passwords to control access.** Only approved users should be able to administer the site and post, and such activity should be trackable. Each student should have a unique login and students must be taught not to share their passwords.
 - **Allow posts to be deleted.**
6. Be prepared to support any opinions or comments that you post. Identify yourself and be a good role model in using the technology.
7. Ensure that your use of language and of students' names is appropriate and in keeping with custom and practice of your school. Insist that your students abide by these customs and practices also.

Netsafe, the internet safety group (<http://www.netsafe.org.nz>), provides a variety of resources, including support and advice, for schools, students, and teachers on keeping safe online.

Their cybersafety guide for schools can be located here:
<http://www.cybersafety.org.nz/kit/welcome/cybersafety.html>

Web 2.0 online safety for teachers

Social networking sites, such as Bebo, Facebook and Oldfriends¹, provide opportunities for teachers to link online with like-minded people sharing ideas and information, as well as providing another forum for communication with students.

Communication online is often informal. It lacks the non-verbal clues of our face-to-face conversations and it is easy to respond and publish before the time has been taken to consider exactly what the communication was about and whether the quick-fire response really was the right one. A particular issue for teachers is that of maintaining appropriate student / teacher boundaries in these more informal forums.

Teachers should be aware that the publication of private and personal information in any online forum cannot be controlled, nor can the use of this information be monitored. Information you have published may be copied, altered and republished on another website or in another format. Search engines cache information and in this way often provide a link to material that the site owner thought they had removed. Injudicious publication of personal information can provide opportunities for dishonest and opportunistic individuals to explore, gather, distribute and manipulate personal information about other people, without their knowledge and/or consent and may provide opportunities for identity thieves.

Be aware that people may associate your online activity with your school or with your job as a teacher.

It is also becoming more common to see employment disputes involving the use or misuse of the Internet, in part because it has become so easy to publish and distribute information, including very personal information and photographs. Employees have been dismissed from their jobs as a result of writing inappropriate or negative comments about their employer or employing organisation online. Recruitment firms and potential employers are now regularly checking candidates by 'looking them up' on Google or searching for their profiles on social networking sites.

So how do teachers keep themselves safe online?

1. Remember activities online affect your life offline.
2. Check your school policy.
3. **Maintain appropriate student / teacher boundaries.**
4. Do not post, in any forum, information you would not feel comfortable sharing with a stranger (including address, phone number, photographs, and party invitations). Don't post embarrassing material.

¹ A list of social networking sites can be found on wikipedia at http://en.wikipedia.org/wiki/List_of_social_networking_websites

5. When using web tools including email, blogs, forums and social networking sites, consider using an appropriate pseudonym and/or email address instead of your full name.
6. Take the time to read about the site you want to post information to. What is the site's privacy policy? What are the terms of use? How does the site deal with misuse?
7. If you want to use a social networking site for communication with students – set one up for this purpose and consider which site (e.g. Myspace, Bebo, Facebook) will be best for this use. Be clear about your goals for the use of this site – see the advice given earlier.
8. Use the privacy tools available on the sites you control, control access; you may want to set privacy parameters to the maximum. Be aware that some social networking applications allow developers access to your information, which may then be made available to other organisations such as marketers.
9. Reconsider the amount of detail you reveal about yourself - and your associates, including colleagues, students and family - online.
10. Protect the privacy of your associates, including colleagues, students and family. Remember that the information you post about them, on your own site and other sites, may be available to people they do not wish to share that information with. This includes photographs.
11. Be careful about accepting friend requests from people you don't know or trust.
12. Have a neutral picture of yourself as your profile image on social networking sites.
13. Before installation of any social networking application check the terms of use and check the developers of the application. Remove social networking applications that you are not using.
14. Do not use the same password for social networking sites as you do for online banking and credit card accounts.
13. Make sure you have anti-virus, anti-phishing and anti-spyware software on your computer that is running and up-to-date!

When others abuse your rights to privacy or publish inaccurate information online what can you do?

1. Ask them to remove the material.
2. Contact the site and request they remove the information (what is the site's grievance procedure?)