

# Social Media @ Work

With more and more cases involving online harassment, bullying, & invasion of privacy coming before FWA, it's important that Union members do all they can to avoid the traps of using social media. The ASU has produced these tips to help keep you safe, and prevent your online networks from becoming evidence against you in the case of a dispute.

## 1. Adjust your privacy settings and review them often

Facebook and twitter default to very public settings for your posts, but you can adjust your settings so that only your friends (or friends of friends) can see them.

In facebook, your settings can be changed by clicking on the "Account" tab in the top right hand corner, and then clicking "Privacy Settings". Click "Custom" in the left hand column to adjust who can see each category of post. Every now and then it is worth coming back to this page to see if facebook's privacy settings have changed.

In twitter, click on your name in the top right hand corner of your home page and then click 'settings'. Click 'protect my tweets' if you want only people you approve to be able to see your tweets. Remember, unless you check this box, your tweets could appear in google searches of your name!

In YouTube, you can customise the privacy settings of each video you post. 'Unlisted' is a particularly good setting, because you can then share the link with just the people you want. Remember though, that you have no control of who your friends choose to share the link with.

## 2. Do not friend your boss

Even if you're quite chummy with your employer or colleagues, adding them to your 'friend' list is fraught with danger. On the other hand, even though you're completely within your rights to do so, it can be hard to turn them down. Thankfully, you have several tactful options.

### *I'll friend you on LinkedIn*

Explain to your boss that you prefer to keep your private life private, but that you'd be very happy to add them as a contact on LinkedIn. LinkedIn is a great networking tool that functions like a business version of facebook. You might even score a written reference out of it!



### *Parallel accounts*

If you're using facebook to contact a lot of colleagues or work contacts or managing the company's facebook page, you may want to set up a separate account for your work persona. It can be very handy if you don't want pictures of Friday night being seen on Monday morning.

### *Limited Profile*

As a last resort, you can add your boss to your 'limited profile' or even manage exactly what they can see on your profile in privacy settings.

### **Close shave for hairdresser**

In late 2010 a young hairdresser was fired for posting a sarcastic comment about her holiday pay on facebook. Fair Work Australia ruled that since she didn't name the employer and no clients saw the post, she should be paid compensation for unfair dismissal, but she was not reinstated. FWA also effectively held up the principle that facebook posts could be grounds for termination.

## 3. If you don't have anything nice to say...

You may think you're just typing letters onto a screen and criticising some silly comment from a username like "tweetdaemon69", but remember, that's (probably) a real person with feelings. If you still want to post a negative comment, consider that it might be read by your boss, your mum, or your parish priest! Even if your posts are protected, what's to stop tweetdaemon from re-posting it on their personal blog, and staining your good reputation?

The same goes for criticising an individual or organisation to a third party or to a forum you think secure. The recipient/s of your comment can always take a screen shot of your post and re-post it publicly. Better to keep it clean.



## 4. NSFW

What sites you visit on your own time is your business (within the law of course), but visiting controversial websites at work is a big no-no. Did you know that your company can find out what sites you've visited from your office computer? Even email attachments you've downloaded or uploaded? They can – someone could even be watching your screen from a remote location!

### **FWA upholds Dairy Farmers email porn sackings**

Fair Work Australia has dismissed as “disingenuous nonsense” union claims that workers sacked for emailing pornography to each other were hard done by because they had not been trained not to send porn at work.

Don't forget that many employers have policies on internet usage that you should be aware of. Beyond this policy, use your common sense and avoid opening un-named links.

On that note, have you ever received a

link described as “**NSFW**”? That stands for “not safe for work”, and the link will probably take you to a site with loud music or other incriminating content.

## 5. Don't give your boss a reason

Companies invest a lot in the reputation of their brand, and so they're not likely to find a group of employees rubbishing the brand particularly funny. If you have a legitimate complaint about your workplace conditions, call your union – we can help! Under no circumstances, and especially not on your union's page, should you name your employer or any brand names in a written comment online. This extends to general complaints about 'work' if you've listed your employer on your profile.

## 6. Wolf in sheep's clothing

Facebook's policy is for people to use real names, but how do you know people are who they say they are? Before you launch into details with an old friend, check their posts, photos, and personal info with a critical eye.

Facebook profiles can also be hacked or taken over by viruses. If a friend you haven't spoken to in a while posts a strange link on your page, think twice before clicking. If your profile is infected with a virus, the same link will be shared with all your friends!

**Questions?** Contact Edwina Byrne,

ASU Media and Communications Officer: [ebyrne@asupsvic.org](mailto:ebyrne@asupsvic.org)

## 7. Customise your privacy settings to your audience

Did you know that you can create lists of your facebook friends? Use this feature to share posts with a select subset of your friends, or to exclude a subset from viewing it. You could make a list for family members, work friends, or even a small group of your best friends. How many of your 100+ facebook friends do you actually trust?

## 8. Don't share your birthday

Everyone loves receiving birthday wishes on their social media account, but it's vital to protect this information. Banks, Insurance firms and other organisations often use your birthday as identifying information, so sharing this with the online world exposes you to identity fraud. Other information in this vein includes your mother's maiden name and the names of pets.

## 9. On holiday?

Counting down the number of days until your holiday is all in good fun, but is it really worth broadcasting the fact that you're house is unoccupied? Post the photos when you get back and save the countdown for your internal monologue.

### **What are you really sharing?**

Social media extracts all sorts of data and metadata when you interact online. For example, when you upload photos, facebook extracts the time, date and place you took that photo. Facebook also knows what other websites you're viewing from your home or office computer.

## 10. Even top privacy settings aren't foolproof

If you work in a highly charged political environment or have influential opponents, be aware that even the tightest security settings can be hacked by a well-caffeinated teenager. Smart phones are particularly susceptible to such attacks, and if you've ever checked your bank balance or paid for something from your smart phone, you could be in real trouble. Simply setting a passcode to access your phone can protect you.

### **Safety Help from Facebook**

Safety Guide

<http://www.facebook.com/help/?safety=general>

Privacy and Data Use Policy

<http://www.facebook.com/about/privacy/>