This fact sheet covers:

- the risks to your organisation involved with using social media
- how to avoid and manage these risks
- whether your organisation can regulate employees’ use of social media, and
- key ways to minimise the risks of social media to your organisation.

Social media provides exciting opportunities for not-for-profit organisations because it has potential to reach a huge audience to whom you can promote your organisation and its activities.

But social media is not without its legal risks. Although it can feel as though social media is unregulated and you can say what you like, the law still applies online.

Postings to a social media site are publications like any other media publication and are subject to the same defamation, discrimination and intellectual property laws and occupational health and safety laws about bullying. There is an added complexity that you may be held to account anywhere in the world where your online publications are downloaded. Liability for social media content may extend to your organisation and those who engage in online activities on its behalf.

What risks does social media pose to our organisation?

When social media is used effectively it works a bit like an online conversation.

Participants can express both positive and negative opinions through the comments posted, creating a rich dialogue on topics of interest. But, as with all conversations, social media communications can get out of hand. For example, if your organisation’s Twitter account is used to attack someone's conduct or beliefs, or make inappropriate comments about a member of your organisation or the public.

You can’t always control the content of posts or tweets, or the speed with which online events can move, so social media may pose a range of risks to your organisation. Particular dangers arise if you allow third parties over whom you have no control and who you may not know or be able to identify, to post material on your website.

Depending on the circumstances, responsibility for defamatory or illegal posts can lie with your organisation as the operator of the site, or with the individual who posted
the content (or both). Whether you are required to monitor posts put on your social media sites is not a settled issue at law. However, we would recommend that if you become aware of an illegal post you should take it down rather than ignore the issue, and if unsure seek further legal advice.

You need to know that:

- information posted is immediately available to anyone who can access the relevant site
- information can be passed on very quickly and spread very fast (it could even ‘go viral’), and
- once something is posted, even if you delete the information or take it down, it might be impossible to ever completely remove it from the internet.

Key risks and their implications

Risk to reputation

Social media can enhance your organisation’s reputation where it’s used strategically and well. It can extend the community’s awareness of your organisation and promote its aims and activities.

On the other hand, when used poorly, social media can damage the reputation of your organisation very quickly, in a far-reaching and potentially permanent way.

Risk to your organisation’s reputation can come from posts on your organisation’s social media sites – both your own posts and posts of others.

EXAMPLE

A post might be added to your organisation’s Facebook page by a member that includes damaging statements about one of your organisation's services.

Risk to your organisation’s reputation can also come from posts on someone else’s social media sites that damage your organisation’s reputation.

EXAMPLE

A volunteer posts a negative comment on their own Facebook page about your organisation's president. The volunteer's Facebook friends include members of the organisation. Membership numbers reduce because confidence in the president is undermined by the comments of the volunteer. Usually this damage occurs because the link between the person and the organisation is clear (ie. they identify themselves as a volunteer, employee or service user).
Risk of breaching copyright

Copyright protects the expression of ideas in material form (eg. text, pictures, music, film/video) – it is an automatic protection that exists when original material is created.

If your organisation posts or uses photos, music, text or other content on your social media sites without copyright permission, your organisation might be in breach of copyright or trade mark laws, even if you are not making any money from the use of the material.

So, if you post material on any of your social media sites and you don’t own the copyright, you need to make sure you have the copyright owner’s permission to use the material (eg. permission from a photographer to use their photos on your Facebook page).

---

**NOTE**

Copyright is a complex area of law. We recommend you read NFP Law’s ‘Guide to Intellectual Property for Victorian Community Organisations’ to learn more about copyright and other intellectual property issues. The Guide is available at [www.nfplaw.org.au/ip](http://www.nfplaw.org.au/ip)

---

Risk of misuse of information and breach of confidentiality

The speed and reach of information through the internet can work to your advantage, but can pose risks to your organisation if material posted is sensitive or inaccurate.

A number of legal consequences can arise if a staff member posts, tweets or uploads sensitive information about:

- their work with the organisation
- the identity or details of people connected with the organisation, or
- the intellectual property of the organisation.

Your organisation could be exposed to legal action, for example for breach of privacy laws, or confidentiality requirements could be breached. Inappropriate posts might also expose your organisation’s intellectual property or trade secrets that could then be used by someone else (for example a competitor).

---

**CAUTION**

Your organisation can be liable for a disclosure made by a volunteer or employee. If, for example, your organisation assists individuals with mental illness, and a volunteer posts information on your organisation’s Facebook page which identifies one of the organisation’s clients and the client suffers a loss as a result, the organisation may be liable for the loss caused by the volunteer's disclosure.

---

Risk of sexual harassment, discrimination and bullying through social media

Social media also provides an avenue through which sexual harassment, discrimination or bullying can occur to staff members of your organisation. If bullying or harassment occurs through social media and there is a sufficient link to the workplace, your organisation may be implicated.
An employer can be held legally responsible (vicariously liable) for the actions of employees and potentially volunteers, unless it can be shown that all reasonable steps have been taken to prevent these actions.

Reasonable steps that employers can take to prevent harassment and bullying from occurring in the workplace include the implementation of written policies and the provision of training on the use of social media in and out of the workplace.

**Risks raised by staff members’ personal social media sites**

It can be tempting to read a potential worker or volunteer’s Facebook page or tweets to learn more about the applicant. However, your organisation must be careful - using such information could lead to a claim of discrimination.

Employers can decide not to employ a person based on something they learn from the applicant’s social media pages, provided that they do not base that decision on an attribute protected by the anti-discrimination laws such as age, gender, ethnicity or disability.

The same rules apply outside the recruitment process. Using information about a staff member that is accessed from their social media sites could lead to claims of discrimination or victimisation in the workplace if the staff member alleges that the information has been unfairly used against them.

**EXAMPLE**

An employer searches an employee’s Facebook page and discovers that the employee is pregnant. The employee has her hours cut and feels discriminated against. The employee realises that the employer has discovered her pregnancy through Facebook and is treating her unfavourably because of this.
How can we minimise the risks of social media?

In summary, the following steps (some of which are explained in more detail below) can be taken to reduce risks associated with social media.

**MINIMISING THE RISKS OF SOCIAL MEDIA**

- Create a clear social media policy.
- Incorporate social media issues into all relevant workplace policies.
- Train and educate workers (employees, contractors and volunteers) about social media and expected standards of behaviour for its use.
- Allocate responsibility or authority to post on social media on behalf of your organisation.
- Be careful when using information from a job applicant or staff member's social media accounts which is not otherwise publicly available.

Have a social media policy

There has been an increase in social media-related decisions by Fair Work Australia. This highlights the growing need for organisations to have a clear social media policy.

**EXAMPLE**

The London Olympics Organising Committee (**LOCOG**) recognised that volunteers at the London Olympics would want to use social media to share their experiences at London 2012. LOCOG therefore provided guidelines to volunteers to give basic advice on ‘interacting in a social media environment’ and to protect the interests of LOCOG’s workforce, operation and sponsors.

Volunteers were warned not to use social media to:
- give away breaking news about athletes
- disclose the location or activities of athletes or celebrities, or
- disclose other sensitive information.

What should a social media policy include?

At the very least, your organisation should promote guidelines for responsible use of social media and outline how offensive or discriminatory comments will be moderated and/or reported.

Ideally, your social media policy should also include:
- a definition of social media
- a description of social media behaviour that is acceptable and unacceptable
- a statement that common sense and decency should dictate online conduct
clear directives about when and for how long workers may use social media sites at work (eg. during breaks, lunch hours, anytime within reason etc)

- a prohibition on employees and volunteers from saying or doing anything on social media that:
  - could bring the organisation into disrepute
  - gives away your organisation’s confidential information or the confidential information of anyone associated with the organisation
  - could be considered derogatory or disparaging by colleagues or clients, or
  - undermines workplace productivity

- a directive that social media must not to be used to discriminate, harass or bully other co-workers

- a statement that hiring decisions are based only on information provided by the applicant, sources provided by the applicant and information publicly available

- a statement that the social media policy applies to remote access to social media using the employer’s IT systems (if applicable)

- a warning that comments made in private accounts out of work hours may result in disciplinary action — that personal posts by employees are not necessarily private and may still be considered related to their work

- a reminder of the risks of social media – that anything posted can be seen by many, quickly and is not easy to erase

- the consequences of breaching the social media policy. Employees and volunteers should be aware of how they will be disciplined if they breach the policy, and

- a recommendation that it is best to avoid being ‘friends’ with colleagues to alleviate issues that arise from inappropriate conduct being linked back to the workplace.

**RECENT CASE**

Fairwork Australia heard a case involving a former employee of the Good Guys, who was frustrated because he had not been paid his commissions. He had his Facebook page set to maximum privacy settings so only his ‘friends’ could see it, but 11 of these ‘friends’ were co-workers. He posted offensive, threatening material about the company and his manager to Facebook. This came to management’s attention and he was dismissed.

Fairwork Australia found his dismissal was reasonable because the employer’s handbook warned employees not to use social media in this way and, even if there had not been a policy, common sense says that writing and publishing insulting and threatening comments about another employee is grounds for dismissal.
Address social media use in other workplace policies

Your organisation should review existing policies, including those on discrimination, harassment and bullying, to ensure that they sufficiently address the use of social media in that context.

Update your IT, OH&S, privacy and confidentiality policies to incorporate social media policies and issues.

Address social media in training and induction

All staff and volunteers must be aware of the organisation’s social media policy, and that there are social media aspects of other workplace policies.

Induction materials and procedures for new workers (volunteers, employees and contractors) should address the use of social media and help workers understand risks and benefits.

Social media should be referred to in any confidentiality agreements signed by staff and volunteers. Confidentiality agreements should identify information that is considered sensitive and confidential and ensure that workers agree not to share such information online without prior consent.

Guidelines and reference materials should be developed to assist staff to understand what is confidential and sensitive and what they can and cannot share via social media platforms. Any regular staff training should include a component on the appropriate use of social media in the work context.

Allocate responsibility for your own organisation’s social media activities

Decide how your organisation will moderate and control your group’s own social media activity. Decide who is responsible for posting and monitoring comments, updates, feedback and keeping your social media sites consistent and accurate.

You may have different authorities for different kinds of posts. For example, posting about events that your organisation is holding may need a lower authority than posts referencing government policy or posts directed to a politician (that may need sign-off from the CEO or board).

You should also allocate responsibility for monitoring comments on your own social media pages. Comments by other people on your own social media pages that breach the law may cause your organisation to also breach the law – so it is essential to take down problematic comments (e.g. comments revealing confidential information, defamatory or harassing comments etc).

It would also be useful to regularly monitor social media and search for disparaging or damaging posts about your organisation, its employees or its clients. While you can delete your own posts, or posts on your own pages, you cannot delete those of other users on their accounts without going through a process with the relevant social media site. If you believe another user is making defamatory comments about you or your organisation, or is breaching any copyright or other intellectual property laws, or the social media platform’s rules, you can report the violations to the platform, which will review the users account and may decide to remove or disable access to the infringing material. You could also contact the person making the posts if you know who they are (but you may want to talk to a lawyer before doing this).
Can our organisation regulate employees’ social media conduct?

Yes, the law allows employers to regulate the conduct of employees on social media. It requires employees or volunteers to be careful about what they post on their personal social media sites.

Your organisation can implement policies that regulate the social media conduct of employees or volunteers in their private time as long as your organisation’s policies are:

- reasonable
- related to the practice of the organisation, and
- related to the employment requirements of the employee.

In some circumstances, your organisation can sack an employee because of the employee’s conduct on social media. Excessive use of social media during work hours may also constitute a valid reason for termination of employment.

RECENT CASE

In a case decided in 2008, 13 Virgin Atlantic Staff criticised the cleanliness of Virgin’s fleet and passengers on Facebook. One post described passengers as ‘smelly and annoying’ and another claimed the planes were full of cockroaches. The employees were dismissed for bringing ‘the company into disrepute’. The airline said that ‘It is impossible for these cabin crew members to uphold [our] high standards of customer service ... if they hold these views.’

Fair Work Australia has held that ‘it would be foolish of employees to think they may say as they wish on their Facebook pages with total immunity from any consequence’ (Commissioner Bissett, Miss Sally-Anne Fitzgerald v Dianna Smith T/A Escape Hair Design [2010] FWA 7358). Comments on social media that relate to work can warrant discipline or dismissal if they damage the organisation.

When considering if an employee’s posts on their personal social media are inappropriate, a range of factors are relevant:

- was the employer named (or can the employer be easily discerned)?
- who can access the comments?
- what was the nature of the social media activity and how serious was it?
- how long were the comments left up?
- what was the effect on the organisation? and
- did the organisation have policies on the use of social media, what did these say, and was the conduct in breach of the policies?

RECENT CASE

Fair Work Australia heard a case where an employee had published comments critical of her employer on Myspace because she was disgruntled about her employer’s investigations into sexual harassment allegations that she had made. She then refused to remove or modify the comments. Fair Work Australia found this to be a valid ground for termination of her employment contract.
Resources

Related Not-for-profit Law Resources

The Not-for-profit Law Information Hub has further resources on the following topics:

- Intellectual Property
- Social Media
- Advertising and communications

Other Resources

- iTaNGO

This is an online tool to help you generate the starting blocks of your organisation's social media policy. The streamlined process requires you to answer a brief questionnaire and provides you with a Social Media Policy customised to your organisational needs.