Social media and your organisation

Legal information for community organisations

This fact sheet covers:

- the most common forms of social media – Facebook and Twitter
- the risks to your organisation from social media use, and
- steps you can take to minimise risks and maximise the benefits of using social media

What is social media?

Social media refers to any form of internet site or app that allows for social networking. It includes sites and apps such as Facebook, Twitter, Instagram and Snapchat. This fact sheet focuses on Facebook and Twitter (the two most popular forms of social media) however, the risks identified and recommendations made to minimise these risks apply to other sites and apps that may be used by community organisations.

Facebook

Facebook has been an incredibly popular social networking service. As early as 2017, there were over 1.86 billion monthly active Facebook users worldwide. Facebook connects people who have signed up to Facebook (users) with other users, events, businesses, causes, not-for-profits and interest groups.

Individual users on Facebook create a 'profile', which includes information about themselves and a 'wall' on which people can make comments. Once a profile is created, users can post onto Facebook and add other users as 'friends'. 'Friends' can see each other's profiles and share stories, photos, video, events and other content.

If you want to set up a profile for your organisation, you can create a 'page' for your organisation. This works in a similar way to an individual profile. When people 'like' your organisation on Facebook this means they see your organisation's page and, if permitted, can write messages and post content onto your organisation's wall.

Facebook also allows organisations to create and join 'groups', to advertise goods and services and to integrate Facebook with other applications. It also provides a number of tools to help you fundraise.

Depending on how a user sets the privacy setting, parts of a profile may be public. This means those parts can be viewed by third parties, such as people who are not 'friends', people who are not Facebook users and the profile (or parts of) may appear in a Google search.

Twitter

Twitter is a social networking service that allows its users to send and read text-based posts of up to 140 characters, known as 'tweets'. The distinctiveness of Twitter is its short format and ability for quick information sharing.

You can create a Twitter account for free by visiting the Twitter website. Once your account is created, you can then manage how you want your account to operate (see 'settings') – for example, making your tweets 'private', deciding if you want to be 'tagged' in photos, adding a location to your 'tweets' and security measures (like verification of login requests).

After setting up an account, you can tweet, retweet and 'follow' other users. If you 'follow' a user, you can see their profile and tweets and can retweet their tweets. Other users can automatically 'follow' you as well, unless you amend your account settings to require 'acceptance' of all followers. Your tweets will be displayed on your profile page, on the profile page of each of your followers and in the general Twitter public timeline (unless you decide to disable this function in your account settings). Some common functions include:

- **Retweet** – Retweeting is a function which allows a user to re-post a tweet made by one of the users they are following. A retweet automatically gives the original tweeter credit for their tweet, as a retweet will appear beginning with the original tweeter's @username.
- **Reply or mention function** – If you want to send a message to a specific user you can send it with @username at the beginning of the tweet. While all your followers can see the tweet, it's understood that the message was intended for that user. You can also simply 'mention' another user in a tweet by using the @username format.
- **#Hashtags** – A #hashtag is used for discussing a topic or keyword. You can search for tweets on a particular topic by searching using a #hashtag. You can also start your own #hashtag for any topic, event or issue you want to discuss.

What risks does social media pose to your organisation?

Social media provides an exciting opportunity for community organisations because it has the potential to allow an organisation to reach a huge audience to promote its aims and activities.

However, social media use also poses a number of risks that your organisation should consider.

So your organisation can maximise the potential benefits and minimise the risks of using social media, it should implement appropriate polices (explained further below).

Postings to a social media site are subject to the same defamation, anti-discrimination and intellectual property laws as other publications, such as newspapers. Postings may also amount to bullying or harassment of your employees, volunteers or others. You may be held to account anywhere in the world where your online publications are downloaded.

There is also the added complexity that, often, other people may post comments on your social media sites. Depending on the circumstances, your organisation may be responsible for defamatory or illegal posts made by others on your social media sites, even if the person who posted the content is also liable (legally responsible).

Note

You (and people that work in your organisation) need to know that:

- information posted is immediately available to anyone who can access the 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 post, it's almost impossible to ever completely remove it from the internet

These risks to your organisation, (explained in more detail below) include:

- risk to reputation
- risk of breaching copyright or other intellectual property rights
- risk of misuse of information and breach of confidentiality or privacy
- risk of defamation

- risks raised by personal social media sites (of employees and volunteers), and
- risks raised by using information from personal social media sites

Risk to reputation

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

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

Risk to your organisation's reputation may come from posts:

- on your organisation's social media sites – both your own posts and posts of others, and
- on someone else's social media site that damage your organisation's reputation

Example – post on your organisation's site

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

Example – post on an external site

A volunteer posts a negative comment on their own Facebook page about your organisation's president. The volunteer's Facebook friends include members of your organisation. Membership numbers reduce because confidence in the president is undermined by the comments of the volunteer.

Usually this type of reputational damage occurs because the link between the person and the organisation is clear (for example, they identify themselves as a volunteer, employee or service user).

Risk of breaching copyright or other intellectual property rights

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

If your organisation posts or uses photos, music, text or other material on your social media sites without permission from the owner of the copyright in that material, 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.

Risk of misuse of information and breach of confidentiality or privacy

The speed that information travels via the internet can work to your advantage, but it can also pose risks to your organisation if material posted is confidential information, personal information or inaccurate.

For example, a number of consequences may arise if an employee or volunteer posts, tweets or uploads:

- confidential information about their work with your organisation
- the identity or details of people who are employed by, or volunteer for, your organisation
- the identity or details of donors, clients or members of your organisation, or
- trade secrets or other intellectual property of your organisation

If this occurs, your organisation could be exposed to legal action, for example, for breach of privacy laws.

Inappropriate posts might also expose your organisation's confidential information that could then be used by someone else (for example a competitor).

Caution

Your organisation could be liable for a disclosure made by a volunteer or employee.

If, a volunteer with your organisation posts information on your organisation's Facebook page which identifies one of the organisation's clients, the organisation may be liable for the volunteer's disclosure.

Risk of defamation

Comments posted on social media may be defamatory. A defamatory statement is an intentional statement about a person that is incorrect and which is likely to hurt that person's reputation.

Again, your organisation could be held legally responsible for posts made by third parties on your site which are defamatory and also for the social media activities of employees and potentially volunteers if these are defamatory, unless it can be shown that all reasonable steps have been taken to prevent these actions.

Related Not-for-profit Law resource

For more information, see our webpage on defamation.

Risks raised by personal social media sites (employees and volunteers)

Comments made on social media by an employee or volunteer have the potential to negatively impact your organisation's reputation or interests or those of your donors, clients or members.

Use of personal social media sites may also result in complaints of sexual harassment, discrimination or bullying of your employees, volunteers or others. If bullying or harassment occurs through social media and there is a sufficient link to the workplace, even if your organisation's social media sites are not used, your organisation may be liable for this.

Related Not-for-profit Law resource

For more information about laws relating to employees and volunteers go to our webpage on 'the people involved'.

See the case examples below of:

- instances of employee's use of personal social media sites,
- the impact on their employment relationships, and
- what the law allows in relation to the regulation of the conduct of employees and volunteers on social media

Case example – derogatory comments on Facebook

In *Remmert v Broken Hill Operations Pty Ltd [2016] FWC 6036*, an employee, Mr Remmert, posted a derogatory comment about a supervisor at the organisation (BHO) on Facebook outside work hours. An investigation by BHO into the post concluded that Mr Remmert's comment intended to belittle and ridicule the supervisor. BHO decided to terminate Mr Remmert's employment.

The Fair Work Commission held that BHO had a valid reason for dismissal. Even though Mr Remmert was home when he posted the comment and the supervisor was not named, because his colleagues could infer that the post was about the supervisor, there was a sufficient connection to his employment. Mr Remmert had also previously received a final warning for similar bullying conduct.

Despite this, the Commission ultimately found that the dismissal was unfair due to a lack of procedural fairness offered to Mr Remmert. The investigation had in part relied on a 'confidential report' relevant to the incident. However this 'confidential report' was not provided to Mr Remmert and he was not given the opportunity to respond to its contents. As a result, the Commission held that his dismissal was harsh and unreasonable.

Case example – act of 'unfriending' on Facebook

In *Roberts v VIEW Launceston and others [2015] FWC 6556*, the Fair Work Commission considered a bullying claim made by Mrs Roberts. One of the bullying allegations was that a fellow employee had 'unfriended' Mrs Roberts on Facebook.

The Commission found that, when considered all together, the majority of the conduct complained about was unreasonable and upheld the bullying claim. It's unlikely that the act of 'unfriending' Mrs Roberts alone would have been considered bullying. However, in all the circumstances of this case the behaviour was found to be unreasonable.

Case example – social media conduct out-of-hours

In *Little v Credit Corp Group Limited t/as Credit Corp Group [2013] FWC 9642*, Credit Corp employee, Mr Little, made Facebook comments about debt counselling charity Christians Against Poverty (**CAP**), an organisation that had dealings with Credit Corp.

Mr Little posted twice on CAP's Facebook page:

- 'For reals bro, you should put a little more of funding into educating consumers on how the world works rather than just weaselling them out of debt, blah blah blah, give a man a fish/teach a man to fish.'
- 'No thanks, just take my advice and try to educate people about things like 'interest' and 'liability' rather than just weasel them out of contracts. #simple.'

Mr Little also posted on his own Facebook page about a new staff member at Credit Corp.

On discovering these comments, Mr Little's employer summarily dismissed him on the basis of serious misconduct. Credit Corp had previously warned Mr Little about his online activities.

Mr Little argued that his social media comments were made in his own time, they were his opinions, and he had not identified himself as a Credit Corp employee. However, the Fair Work Commission held that Credit Corp had lawfully terminated Mr Little's employment.

Even though Mr Little believed he had masked his identity, the Commission found that CAP was able to establish who he was and who he worked for. The Commission also found that the comments made by Mr Little on CAP's Facebook page would likely have had an adverse impact on Credit Corp's relationship with CAP and damage Credit Corp's wider reputation.

This case highlights that social media use can blur the lines between private and work life. In particular, an employee can be held responsible for out-of-hours social media conduct if it impacts on the employment relationship or damages the employer's reputation.

Conduct of employees and volunteers and social media

The law allows you to regulate the conduct of employees and volunteers on social media to a certain extent. Your organisation can implement policies that regulate the personal social media conduct of employees or volunteers as long as your organisation's policies are:

- ✓ reasonable
- ✓ related to the operations of the organisation, and
- ✓ related to the employment or volunteer requirements of the employee or volunteer

In some circumstances, your organisation may dismiss an employee or end a volunteer arrangement because of conduct on social media.

Excessive use of social media during work hours may also constitute a valid reason for dismissal. When considering whether to dismiss an employee (or volunteer) as a result of their personal social media use, a range of factors are relevant:

- Was your organisation named (or can your organisation be easily identified)?
- Who can access the comments?
- What was the nature of the social media activity and how serious was it?
- For how long were the comments posted online?
- What was the effect on your organisation?
- Did your organisation have policies on the use of social media, what did these say and was the conduct in breach of the policies?
- Did your organisation provide appropriate training to support its social media policies?

Case example – employee lawfully dismissed over social media post

In *Mr Damian O'Keefe v Williams Muir's Pty Limited T/A troy Williams The Good Guys [2011] FWA 5311*, a former employee of The Good Guys, Mr O'Keefe, 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 on Facebook. This came to management's attention and he was dismissed.

The Fair Work Commission 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.

Risks from using information from personal social media sites

You may seek to use information that you find from an employee or volunteer's (or potential employee or volunteer's) personal Facebook page, tweets or other social media. But using such information could lead to a claim against your organisation, for example, 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 don't base that decision on an attribute protected by 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's hours are cut and she feels that she has been discriminated against. The employee realises that the employer has discovered her pregnancy through Facebook and is treating her unfavourably because of this.

How can your organisation minimise the risks arising from social media use?

Your organisation can take the following steps (explained in more detail below) to reduce risks associated with social media use:

- allocate responsibility for your organisation's social media activities clearly
- create a clear social media policy
- incorporate social media issues into all relevant workplace policies (for example, bullying, sexual harassment and discrimination policies)
- train and educate employees, contractors and volunteers about social media and expected standards of behaviour for its use
- complying with the rules that apply to specific platforms like Facebook and Twitter
- don't use third party material without consent
- protect the privacy of third parties
- remove content and consider closing accounts

Allocate responsibility for your own organisation's social media activities

Decide how your organisation will moderate and control your own social media activity.

Decide who is responsible for posting and monitoring comments, updates, feedback and keeping your organisation's 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 (the latter type of post may need sign-off from the CEO or board).

You may wish also to consider (subject to resource constraints) allocating responsibility for regularly monitoring social media more generally for disparaging or damaging posts about your organisation, its employees and volunteers and its clients and donors.

Have a social media policy

The ever increasing use of social media highlights the growing need for organisations to have a social media policy.

Unless it can be shown that reasonable steps have been taken to prevent the relevant activities, your organisation may be held responsible for some of the social media activity of your employees and potentially your volunteers, such as posts that bully or harass others.

Reasonable steps that organisations can take include the implementation of written policies and the provision of training on the use of social media in and out of the workplace.

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 on 'interacting in a social media environment' 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

Social media policy – what it should include

- a definition of social media (including but not limited to social networks, blogs and microblogs, podcasts, forums and discussion boards and photo and video sharing sites)
- information on where to find details of those employees and volunteers who are able to conduct social media activities on behalf of your organisation, including who is responsible for posting, monitoring and where necessary removing comments, updates and feedback on your social media sites and keeping your sites consistent and accurate. The policy should make clear that, outside these circumstances, employees and volunteers aren't able to comment or make statements on behalf of your organisation on social media
- a description of the personal social media activities to which the policy applies, which should generally be limited to those that impact on the business of your organisation, the reputation of your organisation or the employees and volunteers and other people associated with your organisation
- a requirement that all social media comments be professional and respectful, as applies in the case of all other communications
- a prohibition on employees and volunteers from doing anything on social media that:
  - discriminates against, harasses or bullies other employees, volunteers or others

  - could bring the organisation into disrepute
  - gives away your organisation's confidential information or trade secrets or the personal or confidential information of anyone associated with the organisation
  - is defamatory, or could be considered derogatory or disparaging, of other employees or volunteers or the donors, clients or members of your organisation, or
  - undermines or disrupts workplace productivity
- if your organisation uses internal social media platforms, such as Yammer, rules about use of those internal sites
- a reminder of the risks of social media – that anything posted can be seen by many, quickly and is almost impossible to erase
- a statement that the social media policy applies to remote access to social media using the employer's IT systems
- clear directives about when and for how long employees and volunteers may use social media sites for personal purposes at work (for example, during breaks, lunch hours, before and after standard working hours)
- how compliance with the social media policy will be monitored and the consequences of breaching the policy, and
- references to other policies that impact on social media use

The policy should also specify how it relates to your organisation's other policies, such as your IT and email use, occupational health and safety, privacy and confidentiality policies.

Tip

There are on line tools, like improveIT that can 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.

Case example – the need for a well-drafted social media policy

The importance of having a well-drafted social media policy that is effectively communicated to employees and volunteers was highlighted by the *Fair Work Commission in Glen Stutsel v Linfox Australia Pty Ltd [2011] FWA 8444* (a decision upheld by the Full Federal Court in December 2013).

Linfox Australia sacked employee Mr Stutsel for making racist and sexist comments about two of his managers on his Facebook page. The Commission found that there was no valid reason for Mr Stutsel's dismissal because the employer didn't have a social media policy.

Social media policy – personal social media activities

A key element of your social media policy is providing your employees and volunteers with certainty about your expectations regarding their personal social media use.

Your social media policy should generally only apply to activities that impact on your organisation's business, your organisation's reputation or the reputations of your employees, volunteers and other people associated with your organisation.

Where claims of bullying, harassment or discrimination by means of social media are made by an employee or volunteer, the reasonable steps that an organisation has taken to prevent such activities in their workplace will be assessed. Therefore, your organisation's social media policy, and the steps that you take

to train your employees and volunteers regarding your requirements, may be important in limiting your liability in such a case.

Your policy should:

- set out the circumstances in which an employee or volunteer is authorised to make reference to you as their employer in their personal activities, and
- make clear that, in using social media in their personal capacity, employees and volunteers may not either directly state, or infer, that they are representing you

In addition, a number of the general rules in your social media policy will apply to both an employee's or volunteer's work related and personal social media use. These include for example, as listed in the previous section, a prohibition on using social media in a way that discriminates against, harasses or bullies other employees, volunteers or others or that could bring the organisation into disrepute.

As noted above, your policy should also state when and for how long employees and volunteers may use social media sites for personal purposes at work.

Case example – breach of a social media policy

In *Nirmal Singh v Aerocare Flight Support Pty Ltd [2016] FWC 6186*, the Fair Work Commission considered an unfair dismissal claim relating to comments posted on Facebook.

Mr Singh, a casual baggage handler for Aerocare, was dismissed on the basis that his posts on Facebook breached the company's social media policy.

That policy provided that employees must be respectful of the company, other employees, customers, partners and competitors in social media use and employees were discouraged from using social media in a way that may cause harm to Aerocare.

Aerocare claimed that Mr Singh had posted comments on Facebook that supported Islamic extremist views. The Commission found that the posts were intended to be sarcastic and had not been properly investigated. As a result, the claim for unfair dismissal was upheld. The Commission, however, didn't indicate that it had any concerns with the terms of Aerocare's social media policy itself.

Case example – excessive social media use in the workplace

Fair Work Australia considered excessive social media use during working hours in *Richard O'Connor v Outdoor Creations Pty Ltd [2011] FWA 3081 (24 May 2011)*.

Mr O'Connor was dismissed on the basis that there had been a serious decline in his productivity, with allegations made by his employer that he had used 'Google chat' more than 3,000 times in the three months leading up to his termination. The dismissal was found to be unfair on the basis that the employer could not provide evidence to substantiate its claims, but Fair Work Australia did state that, provided an employee is first notified of the employer's concern and given an opportunity to respond, excessive use of social media may be a valid reason for terminating an employee.

Social media policy - administration rights

When setting up your social media policy, consider carefully who should have administration rights for your social media accounts.

A question often asked is – what should be done when an employee or volunteer has set up an organisation's Facebook page and leaves without providing the details to access the administration page for the organisation to another employee or volunteer?

Unfortunately, Facebook's stated policy is that it won't interfere in such circumstances and won't provide the organisation with access to the administration page. If it's not possible to access the administration page for your Facebook account, you will need to create a new Facebook page. You can then report the original page to Facebook as an 'impersonating account' and Facebook should remove the original page. For this reason, we recommend that you ensure that at least two employees (or volunteers) have an administration role for your Facebook page.

Address social media use in other workplace policies

Your organisation should review existing policies, including those on discrimination, harassment and bullying, IT and email use, occupational health and safety, privacy and confidentiality, to ensure they:

- are consistent with your social media policy, and
- sufficiently address the use of social media

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 volunteers, employees and contractors should address the use of social media and help them understand the risks and benefits of social media use. Any regular staff training should include a component on the appropriate use of social media in the work context.

Supplementary guidelines and reference materials should be developed to assist staff to understand what material relating to your organisation they can and can't share via social media platforms.

Comply with the rules

When you sign up to a social media site, you are usually required to agree to comply with certain terms and conditions. In some cases you can also set rules that third parties must comply with when they visit your site or post material to your site.

Facebook rules

Facebook requires that users agree to a 'Statement of Rights and Responsibilities'. This Statement includes rules about what can be posted, what conduct is prohibited, what happens if you delete your account (or Facebook stops you using it) and other commitments you must make. There are also separate guidelines, for example, that set out the policies that apply to advertisements placed on Facebook and on how to use the Facebook logo.

Tip

Read Facebook's Statement of Rights and Responsibilities before you sign up!

If you already have a Facebook account, you should review the Statement from time to time because the terms and conditions sometimes change.

Rules you can set for your Facebook page

You might want to set up special rules for your Facebook page (called 'house rules').

House rules set out terms of use for people that contribute to your page. These rules should include a statement that users agree to be bound by your rules if they use, 'like' or contribute to your page.

Terms you might consider including in your rules are:

- No text, images, videos, sound or other material should be posted unless it's the contributor's own creation or the contributor has the right to post that material
- A link to another person should not be posted unless the contributor has obtained the consent of the other person

- No material or comments that are defamatory or offensive, infringe the rights of others (including intellectual property rights), are false, misleading or deceptive or otherwise breach any law should be posted
- Any postings by contributors may be re-used by your organisation in any other forum without the consent of the contributor
- Your organisation is not responsible for contributors' posts
- Your organisation has a right to delete any material or posts which it believes, in its absolute discretion, to be:
  - defamatory or offensive
  - an infringement of the rights of others, including an infringement of copyright, moral rights or trade mark rights
  - false, misleading or deceptive
  - confidential information, or
  - otherwise contrary to the intentions, purposes or values of your organisation

Where you have given permission to third parties to write messages and post content on your organisation's Facebook page, you will not be able to control what is posted. However, you can take some steps to protect your organisation in relation to third party material. These steps including having 'house rules', selecting appropriate privacy and account settings and, in some cases, removing material and posts.

Twitter rules

When you sign up to Twitter, you agree to the 'Terms of Service' (Terms).

The Terms outline:

- who is responsible for the content displayed
- who owns and has a right to use the content you submit, display or post (tweet)
- rules about the content you can post and what and who can remove it
- rules about the general use of the service and other commitments you must make when signing up

The Terms also include rules about the use of the Twitter logo, trade marks, domain names and other distinctive brand features.

Tip

Read Twitter's Terms before you sign up!

If you already have a Twitter account, you should review the Terms from time to time because the Terms sometimes change.

There are also Guidelines for the Use of Tweets in Broadcast or Offline Media which include rules on the publication, broadcast or delivery of tweets through any media platform.

Privacy and account settings (Facebook, Twitter and other accounts)

All social media services provide for you to manage your privacy and account settings, and these can be used to provide protection to your organisation.

For example, in the case of Facebook, when setting up your profile page, you may consider implementing some of the following measures:

- adjust your privacy settings so that only those who 'like' your organisation can view the content on your page
- receive email notifications when users have posted comments to your wall. Then you know when things are posted and can see if the comments need to be taken down, and
- activate the profanity block-list to block words you do not want posted on your page

If you don't want (or don't have the resources) to monitor posts regularly, consider disabling users from posting content on your Facebook page. You can do this via your settings.

You should also consider uploading images in low resolution (to make it more difficult for users to copy them) or with a watermark (to protect your copyright).

In the case of Twitter, you may consider implementing some of the following measures:

- adjust your privacy settings so that only those who you approve will receive your tweets
- prevent others from tagging your organisation in photos or sending you direct messages, and
- use the blocked account functions if there are Twitter account holders that you don't want to follow you or view your profile

Tip

If you want to receive opinions on a topic or issue important to your organisation, consider using the Poll application rather than inviting open-ended discussions. This will mean you get a straight answer rather than inviting space for disparaging comments. Of course, there may be times when you want to promote robust public debate on an issue – in which case, a closed-question Poll may not be your preferred approach.

Obtain consent to use third party content

Copyright

If you post or tweet someone else's material you need to make sure you are not breaching someone else's copyright.

Generally the only circumstances in which you won't need consent to use someone else's material are:

- where you use an extract or quote from someone else's writing but you don't use a 'substantial part' of the work. What is a 'substantial part' of a work is a complex legal issue – even if you are just using a small proportion of the work it could still be a 'substantial part' if it is a distinctive, important or essential part of the overall work. For more information see the Australian Copyright Council's fact sheet, 'Quotes and Extracts', or
- if you can rely on one of the 'fair dealing' exemptions in the *Copyright Act 1968* (Cth) (**Copyright Act**). 'Fair dealing' exemptions include use for the purpose of criticism or review, reporting news, research or study or parody or satire. For more information see the Australian Copyright Council's fact sheet, 'Fair Dealing: What can I use without permission?'.

If it would be acceptable to provide a URL link in a publication, then generally it will be acceptable to post that URL link or provide that URL link over Twitter, as long as it's clear where users are being directed, and who owns the content (for example, linking to a publicly available article on another website).

Related Not-for-profit Law resource

Intellectual property, including copyright and trade marks, is a complex area of law.

For more information about these issues, see Not-for-profit Law's 'Guide to Intellectual Property'.

Trade marks

You should also consider – are you posting or tweeting information, images or logos which include someone else's trade mark?

A trade mark is a mark or sign which is used to distinguish goods or services of one person or organisation from those of another. A trade mark may include, for example, a word, phrase, logo, sound, shape, picture or any combination of these.

You should also make sure any trade mark you use on social media is not substantially identical or deceptively similar to another trade mark that already exists.

You can use someone else's trade mark to refer to or discuss another organisation, but you can't confuse the reader into thinking that you are the organisation that owns the trade mark, or that you have an association with, or are endorsed by, them.

Can you link to other websites?

Yes, but be careful!

You might be liable for copyright infringement by authorising use or access to protected material by linking from your page or tweet to infringing material. Generally, you can provide hyperlinks from your Facebook page or a tweet to another website's home page containing copyrighted material as long as it is clear to the user that they are going to another website.

Tip

Sometimes 'deep linking' (linking to a specific page within another website, and not the homepage) may require the website owner's permission. If a deep link allows a user to bypass a copyright notice or terms and conditions, or access restricted material by bypassing technological protection methods, then you should get consent to avoid infringement.

Do you need to attribute work to the creator?

Yes, in general if you are posting or tweeting someone else's work, you must attribute the creator to the work and not treat the work in a derogatory way – even if the creator no longer owns the copyright or you have permission to use the work.

However, where it's 'reasonable' not to attribute a creator to the work, or to treat the work in a way that is derogatory, it will be okay for you to do so. In working out what's 'reasonable' you should consider the nature of the work and how it is being used, as well as the practicalities such as finding the creator. For example if you make a number of attempts to find out who the creator of a work is but can't do so, then it would usually be reasonable to post the work without attribution.

Further comments regarding Twitter are set out below.

Re-tweeting or copying another user's tweets

Twitter's Terms provide that a person who posts content will own the copyright in that content. Whether copying another user's tweets could constitute copyright infringement is not a settled issue. The question is whether a 140 character tweet can be considered an 'original literary work' that will receive copyright protection under the Copyright Act.

Most tweets are unlikely to receive copyright protection because of:

- size – short words, single phrases and titles are less likely to be considered substantial enough to constitute a 'work' and qualify for copyright protection
- content – facts are not protected by copyright law, and
- originality – for copyright protection to apply, a degree of originality or intellectual or creative effort needs to be established, which again is difficult to prove with a single phrase or few words

However, this is an issue which hasn't been tested at law. We, therefore, suggest taking care and considering the relevant issues before reproducing someone else's tweet as your own.

Retweets are unlikely to breach copyright law as retweeting is a function of Twitter and it is known and accepted by users that anyone who posts a tweet is giving their followers the ability to share that content using a retweet. A retweet also appropriately identifies the original tweeter.

Reproducing a compilation of tweets

If you are reproducing a collection of tweets, taken as a whole, then there is a greater chance that the criteria for copyright protection may be satisfied. Copyright can subsist in original compilations and an arrangement of tweets (which has a greater number of words and more original content than one tweet by itself) could be considered an 'original literary work' and be protected by copyright law.

It's unclear whether copyright will be infringed if you are reproducing replies or mentions (@username) or #hashtags.

It could be argued that by using a #hashtag or @username in a tweet, the user (who owns the copyright in that tweet according to the Terms) is giving the #hashtag creator or the user permission (an implied licence) to re-publish or use that tweet.

As the legal position is unclear, we (again) suggest taking care and considering all relevant issues.

Protect privacy

Often you will want to use photos or videos of people on your social media site. Privacy laws are complex, and which laws apply will depend on your type of organisation and circumstances in which the picture or video was taken.

In some cases, where the photos or videos are taken for that purpose, it's legal to post photos or videos on Facebook or other social media sites without the consent of the people shown. But often a privacy notice will still need to be provided to those people.

So, in general, we recommend that if you want to take photos or videos (for example, at an event) and post these on any social media site, you take reasonable steps to ensure that anyone identifiable consents to you using their image on your page.

There are various ways you can get consent from people whose image you want to use (either in photos or videos). For example you can:

- tell people when you are taking their photo or filming that the images may be used to promote your organisation, unless they object
- put a condition on the ticket or invitation for an event which says something like: 'Please note photographs and videos will be taken at this event. By [purchasing or accepting] this ticket, you consent to your image being used for our organisation's purposes, unless you notify us otherwise by [state how your organisation can be notified]', or
- put signs up at the entrance to an event, stating that photographs and videos will be taken and may be published. Provide contact details in case someone wants to notify your organisation that they don't want their image displayed.

If you get consent to use someone's image for a particular purpose (for example, to post on Facebook), but then decide you want to use it for another purpose (for example, for a commercial publication), you will need to get that person's consent to use their image for that broader purpose, unless they would reasonably expect you to use their photo for this other purpose.

Related Not-for-profit Law resource

For more information, see our privacy guide.

Removing inappropriate material or posts and closing accounts

Removing material

Of course, ultimately, you can remove material or posts from your social media accounts if you consider that it might be damaging to your organisation's reputation or might breach any laws, including in relation to defamation, anti-discrimination or intellectual property.

While you can delete your own posts or tweets, or posts on your own pages, you can't directly delete those of other users on their accounts.

If one of your employees or volunteers has made any such posts or tweets (and this is contemplated by your social media policy), you may require that the person removes the post or tweet.

If you believe another user has made such posts or tweets, you can report the violations to the relevant social media platform, which should review the user's account and may decide to remove or disable access to the 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).

Tip

If other users can post content to your organisation's page, then you should regularly monitor your page and delete content or posts which:

- are defamatory or offensive
- infringe the rights of others, including copyright, moral rights or trade mark rights
- are false, misleading or deceptive are confidential, or
- are contrary to the values of your organisation

Tip

If you believe another user of Facebook or Twitter is making defamatory comments about you or your organisation, or is breaching any copyright or other intellectual property laws or the Terms, you can report the violations to administrators of Facebook and Twitter, who will review the user's account and may decide to remove or disable access to the infringing material.

Facebook and Twitter administrators may also suspend and warn repeat violators and, in more serious cases, permanently terminate user accounts.

Closure

If your Facebook page or Twitter account becomes overrun by inappropriate posts, tweets or tags, or your organisation decides that it no longer wants to maintain a presence on that platform, you can deactivate your account. For assistance with this, see the Facebook help centre section on the Facebook website or the Twitter help centre section of the Twitter website.

Resources

Not-for-profit Law resources

- Intellectual Property
- Advertising and communications
- Privacy

Related Legislation

- *Copyright Act 1968* (Cth)
- *Privacy Act 1988* (Cth)

Other Resources

- ImproveIT

  This site has 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.

- Australian Copyright Council

  The Australian Copyright Council has several useful resources located in the Find an Answer section of the website including 'An Introduction to Copyright in Australia', 'Quotes and Extracts' and 'Fair Dealing: What can I use without permission?'.

- Arts Law Centre of Australia

  The Arts Law Centre of Australia provides legal advice and information on a wide range of arts related legal and business matters.

- IP Australia

  IP Australia is a government body that administers Australia's intellectual property rights system (excluding copyright).