Social media and your organisation

Legal information for community organisations

This fact sheet covers:

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

Disclaimer

This fact sheet provides general information about social media. This information is a guide only and is not legal advice. If you or your organisation has a specific legal issue, you should seek legal advice before deciding what to do.

Please refer to the full disclaimer that applies to this fact sheet.

What is social media?

Social media refers to any form of internet site or application that allows for social networking.

It includes websites and applications such as Facebook, X (previously called Twitter), Instagram, YouTube, TikTok, LinkedIn and Snapchat.

Social media provides an important tool 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 risks that your organisation should consider.

The most common social media platforms

This fact sheet focuses on Facebook, X, Instagram and TikTok (four of the current popular social media platforms). However, the risks identified and the recommendations we make to minimise these risks apply to other sites and applications that community organisations may use.

Facebook

Facebook connects people who have signed up with 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 post 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’ or ‘follow’ your organisation on Facebook this means they see your organisation’s page, receive updates about information that your organisation posts and, if permitted, can write messages and post content onto your organisation’s wall.

Individual users and organisations can also create events which can be used to invite specific users or the general public to a specific place at a certain time, for a specific reason.

X

X (previously called Twitter) is a social networking service that allows its users to send and read short message of up to 280 characters (previously known as 'tweets').

Your messages (also called tweets or posts) are displayed on your profile page, on the profile page of each of your followers and in the general X public timeline (unless you decide to disable this function in your account settings).The distinctiveness of X has been its short format and ability for quick information sharing.

Instagram

Instagram is a social network that permits users to take, edit and publish photos and short videos.

Users can add captions and hashtags to describe content which can then be shared with followers through a post, timed story or video reel. Once you post a photo or video on Instagram it appears on your individual profile and will be seen in your followers’ Instagram feed. Timed stories are only available for 24 hours. Instagram allows users to interact with each other through a like, reaction, comment and messaging system.

TikTok

TikTok is a video sharing social media application, where users create, publish, share and watch short form videos which range from three seconds to 10 minutes.

Like other social media platforms, you can follow other users on TikTok if you want to see their video content in your feed. The main feature of TikTok is the ‘for you’ page which features a curated feed of videos based on the content you have engaged with. TikTok has gained immense popularity for its wide range of content, including viral dance challenges, comedy sketches, cooking tutorials and fitness and health tips.

What risks does social media pose to your organisation?

While social media is a useful communication tool, social media use also poses risks that your organisation should consider.

Risks that social media poses to your organisation include:

- risk to reputation
- risk of breaching copyright or other intellectual property rights
- risk of misuse of information and breach of confidentiality
- risk of defamation
- risks raised by personal social media (of employees and volunteers)
- risks relating to data security
- risk relating to use of personal information

These risks are considered in more detail below.

Your organisation should implement appropriate polices to maximise the benefits of using social media and help mitigate the risks of using social media.

Note – laws apply to social media posts

Posts on social media are subject to the same defamation, anti-discrimination and intellectual property laws as other publications, such as newspapers.

Social media posts may also amount to bullying or harassment of your employees, volunteers or other people.

You may be held to account anywhere in the world where your online publications are downloaded.

There is also the added complexity posed by comments that other people post 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

Organisations that operate social media pages may be able to rely on a ‘digital intermediary’ defence for third-party posts in most Australian jurisdictions, provided they meet relevant statutory conditions. As this defence is conditional and not available across all jurisdictions, organisations should continue to monitor their social media pages and promptly address any potentially defamatory or unlawful content.

Case example – responsibility for comments made on an organisation's Facebook page by its users

In *Fairfax Media Publications Pty Ltd v Voller [2021] HCA 27*, the High Court considered whether Fairfax Media Publications was responsible for comments posted by other parties on its Facebook page.

The case was started by Dylan Voller who was abused and mistreated in the Northern Territory's Don Dale Juvenile Detention Centre. Fairfax Media Publications covered his story and posted news articles on their Facebook page. Users of the Facebook page left alleged defamatory comments on the articles. Mr Voller took legal action against Fairfax Media Publications arguing that they were responsible for allowing Facebook users to leave alleged defamatory comments on the Facebook page.

The High Court held that Fairfax Media Publications was responsible for 'publishing' the comments made on its Facebook page by Facebook users – even though Fairfax Media Publications didn't write the comments, approve them or read them before they were posted.

You (and people that work in your organisation) must be mindful 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 it's deleted, it's almost impossible to ever completely remove it from the internet

Risk to reputation

Social media may enhance your organisation's reputation if 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

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).

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 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.

For more information about intellectual property law, see our guide to intellectual property law.

Risk of misuse of information and breach of confidentiality

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

For example, 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 obligations of confidentiality or secrecy.

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

Note – tort of serious invasions of privacy

On 10 June 2025, under an amendment to the *Privacy Act 1988* (Cth), an individual has a cause of action for serious invasions of their privacy in circumstances where there has been an intrusion on their seclusion, or misuse of their information where they had a reasonable expectation of privacy.

The introduction of the new tort addresses longstanding concerns regarding gaps in Australia's privacy laws around rapid advances in information, storage, surveillance and other relevant technologies, as well as changing community perceptions of privacy and the extent to which it should be protected.

This new tort provides an avenue for people who are affected by an invasion of privacy (which might fall outside the scope of the Privacy Act). It is intended to be an independent provision from the Privacy Act and should be interpreted separately.

To be successful in a claim of serious invasion of privacy, the individual must establish:

- an invasion of privacy: intrusion upon seclusion or misuse of information
- a reasonable expectation of privacy in all the circumstances
- the invasion of privacy was intentional or reckless
- the invasion of privacy was serious, and
- the public interest in privacy outweighs any countervailing public interests

The introduction of this tort makes it even more important for organisations to consider carefully the information shared online.

Using photos and videos of members of the public

Organisations will often want to use photos or videos of people on their social media sites. Take reasonable steps to ensure that anyone identifiable consents to the use of their image.

You can get consent from people whose image you want to use (either in photos or videos) by:

- telling people when you are taking their photo or filming that the images may be used to promote your organisation unless they object
- putting a condition on the ticket or invitation for an event, stating that photographs and videos will be taken and may be published, or
- putting up signs 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.

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.

The High Court confirmed, in the Voller case discussed above, that an organisation can be responsible for comments posted by other parties on its Facebook page.

Note – interplay between privacy and defamation law

While the tort of serious invasions of privacy and defamation are distinct areas of law, organisations may find that the issues (and claims) overlap. For example, several defences for the tort (such as absolute privilege, publication of public documents, and fair report of proceedings of public concern) find their origins in defamation law. In addition, the inclusion of public interest is a theme across both areas of law. In defamation law, public interest is a defence. In the tort, public interest is an element.

Despite the overlap, there are important differences:

- the tort seeks to protect a person's privacy, whiles defamation law seeks to protect a person's reputation
- the tort does not require information to be published and if a defendant is found to have invaded the plaintiff's privacy by misusing information that relates to the plaintiff, it is immaterial whether the information was true

Case example – difference between privacy and defamation law

In the landmark decision in the UK regarding the misuse of private information of *Campbell (Appellant) v. MGN Limited (Respondents)* [2004] UKHL 22, the House of Lords accepted that Naomi Campbell (a famous supermodel) had a reasonable expectation of privacy in relation to details of her treatment for drug addiction which had been published without her consent in a newspaper. In this instance, Ms Campbell was not denying she was being treated for drug addiction. As such, her primary claim related to a breach of privacy, and a claim for defamation was not applicable in these circumstances.

[**Note** that the UK does not have a statutory tort for serious invasions of privacy. However, there is a common law tort for the misuse of private information.]

For more information, see our webpage on defamation.

Risks raised by personal social media (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.

Misuse 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.

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

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 – 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 Roberts. One of the bullying allegations was that a fellow employee had 'unfriended' 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' Roberts alone would have been considered bullying. However, in all the circumstances of this case the behaviour was found to be unreasonable.

Case example – derogatory comments on Facebook

In *Remmert v Broken Hill Operations Pty Ltd [2016] FWC 6036*, an employee, 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 Remmert's comment intended to belittle and ridicule the supervisor. BHO decided to terminate Remmert's employment.

The Fair Work Commission held that BHO had a valid reason for dismissal. Even though Remmert was at home when he posted the comment and the supervisor was not named, because Remmert's colleagues could infer that the post was about the supervisor, there was a sufficient connection to his employment. 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 Remmert. The investigation had in part relied on a 'confidential report' relevant to the incident. However this 'confidential report' was not provided to 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.

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 – 'out-of-hours' conduct on social media

In *Corry v Australian Council of Trade Unions T/A ACTU* [2022] FWC 288, Corry had been summarily dismissed by the Australian Council of Trade Unions (**ACTU**) after making a series of highly offensive and discriminatory Facebook posts and comments. Corry argued that the ACTU social media policy did not apply to his out of hours conduct.

The Fair Work Commission examined the Facebook posts and found that Corry's conduct breached various ACTU policies and was contrary to the ACTU's public position.

The Commission concluded that Corry's behaviour was serious misconduct and a valid reason for his dismissal. The ACTU's decision to dismiss Corry for his out of hours conduct on social media was upheld.

In making the decision, the Commission said:

> *A right to hold and express a strongly held views does not however mean the Applicant has an unqualified right to publicly espouse views that are contrary to the interests and values of his employer* [142].

Risks from using information from personal social media sites

Your organisation might 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.

An employer 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.

Risks relating to data security

With cybercrime and data breaches resulting from malicious or criminal attacks on the rise, use of social media poses a significant threat to organisations.

If your organisation has a social media account, it may be at risk of being exposed to a cyber-attack through either direct hacking, phishing or malware.

If a hacker accesses your organisation's account credentials, this may lead to the unauthorised access and distribution of confidential data. This could be damaging for organisations – causing disruption to operations, substantial reputational harm and most importantly, an erosion of public trust.

Effective data security measures are fundamental to safeguarding data and other types of information from cyber-attacks. If your organisation is using social media, you should implement practises to maintain and secure your accounts. This may include:

- setting strong user passwords and multi factor authentication
- implementing and updating security software
- raising awareness through security and privacy training
- developing a cyber security policy

For more information about cybersecurity, see our fact sheet on cybersecurity.

Risks from use of personal data

Organisations can collect various types of personal data about individual users through their social media platforms. The most common types of data that may be collected include basic profile and demographic data (such as gender, age, location), interests and preferences, behavioural data, connection ('friends') lists, advertisement engagement data and user generated content.

If your organisation is collecting personal data through its social media platforms, you must respect user privacy settings and handle personal data in accordance with the relevant laws and regulations.

Some community organisations, including those with revenue over $3 million, and those that have contractual arrangements with government (for example, under funding agreements) may be required to comply with privacy laws. These laws regulate how personal data is collected, stored, accessed, used and disclosed.

It's best practice to assume that all privacy laws apply to your organisation. It's also important to note that there are privacy laws at both state and federal levels

Putting adequate privacy protection policies, procedures and practises in place, will help your organisation and can minimise the risk of personal data being mishandled.

Case example – misleading consumers about personal data

In the Federal Court of Australia case *ACCC V Google LLC* (No 2)[2021] FCA 367, Google LLC was ordered to pay $60 million in penalties for making misleading representations to consumers about the collection and use of their personal location data on Android mobile phones between January 2017 to December 2018.

This case illustrates the ACCC's willingness to initiate enforcement action against companies that mislead users about how their data is collected, stored and used.

For more information about privacy laws, see our webpage on privacy laws.

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 X
- not using third party material without consent
- protecting the privacy of third parties
- removing risk content and consider closing accounts if they can't be managed safely

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 need for organisations to have a social media policy.

Unless your organisation can show it has taken reasonable steps to prevent the relevant activities, it may be held responsible for certain 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.

The 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 – your organisation's policy 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 authorised 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 – this should generally be limited to those activities that impact your organisation's business, your organisation's reputation of the reputation of the employees, volunteers and other people associated with your organisation	☐
• a requirement that all social media comments be professional and respectful (applicable to 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 Slack, 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

Online tools, like improveIT, can help you develop your organisation's social media policy.

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).

Linfox Australia terminated an employee (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 Stutsel's dismissal because the employer didn't have a social media policy.

Case example – the importance of training employees on your social media policy

In *Martin Pelly v Ventia Australia Pty Ltd T/A Ventia* [2023] FWC 907, Pelly filed an application with the Fair Work Commission seeking reinstatement and backpay for an alleged unfair dismissal.

Pelly was dismissed by Ventia for posting sexually explicit content and bullying work colleagues in a private Facebook group named 'Sickos Videos'.

In deciding to reinstate Pelly's employment, the Commission considered (among other things) evidence that Pelly was not provided sufficient training to allow him to have a clear understanding about Ventia's expectations in relation to private social media communications and how they may be perceived to be conduct that is relevant to the employment relationship.

Distinguishing between personal and organisational social media

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 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. Your organisation's social media policy, and the steps 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 refer 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, some of the 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 above, 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 Facebook posts.

Singh, a casual baggage handler, was dismissed on the basis that his posts breached Aerocare's social media policy and appeared to express support for Islamic extremist views.

Aerocare's social media policy required employees to use social media responsibly and not damage the employer's reputation or relationships.

The Commission accepted that the conduct was inappropriate and potentially capable of constituting a valid reason for dismissal. However, it held that the dismissal was harsh, unjust and unreasonable, principally because the employer failed to afford procedural fairness, including by not adequately investigating the context of the posts or properly considering Singh's explanation.

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)*.

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, carefully consider who should have administration rights for your social media accounts.

A Facebook example

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

Facebook's 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 on social media platforms.

Comply with social media platform 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. Before signing up to a social media platform, you should make sure you're familiar with the relevant terms of service.

Tip

Read a social media platform's term of service before you sign up.

If you already have an account, review the terms from time to time because they sometimes change.

Rules you can set for your Facebook page

To prevent harmful or negative comments being published on your Facebook page, you may wish to set up special rules for your Facebook page (called 'house rules').

House rules are usually included in the 'about' section of your Facebook page which sets out the 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.

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.

Use the privacy and account settings on social media platforms

All social media services allow you to manage your privacy and account settings, and these can be used to protect to your organisation.

For example, in the case of Facebook, when setting up your profile page, 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 (so 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 in 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 X, 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, 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, or
- if you can rely on one of the '**fair dealing**' exemptions in the *Copyright Act 1968* (Cth) (**Copyright Act**)

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'

'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 on a social media platform, 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).

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

For more information about these issues, see our guide to intellectual property.

Trade marks

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, this may be acceptable. In working out what's 'reasonable' consider the nature of the work and how it is being used, as well as practicalities such as finding the creator. For example if you make attempts to find out who the creator of a work is but are unsuccessful, it would usually be reasonable to post the work without attribution.

Further comments regarding X are set out below.

'Re-tweeting' or copying another user's 'tweets'

X's terms provide that a person who posts content will own the copyright in that content. Whether copying another user's tweets (or posts) could constitute copyright infringement is not a settled issue. The question is whether a 280 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 issue hasn't been tested at law. We, therefore, suggest you take care and consider the relevant issues before reproducing someone else's tweet as your own.

Retweets (or reposts) are unlikely to breach copyright law as retweeting is a function of X and it's 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.

Removing inappropriate material or posts and closing accounts

Social media can often be used as a platform for disgruntled employees, aggrieved customers, and trolls to post nasty or offensive content which may damage your organisation's online presence and impact public perception of your organisation.

While you can delete posts on your social media pages, you can't delete people's posts on their accounts.

If an employee or volunteer posts on social media, in contravention of your social media policy, you may ask the person to remove the post.

If you believe another user has posted unfavourable content, first review the relevant social media platform's terms of use policy to determine if there has been a violation of the terms. Also collect evidence of the harmful content to help build context and support your claim.

Report any terms of use violations to the social media platform where the content was posted. Once the platform has reviewed the content, they may remove it straight away and possibly block or disable the person who posted the material.

Unfortunately removing the offensive content is not always guaranteed. Often it will be discretionary for the platform to remove the material. If you are still concerned, seek independent legal advice.

Tip

If other users can post content to your organisation's page, 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

If one of your social media accounts becomes overrun by inappropriate posts, comments or tags, or your organisation decides that it no longer wants to maintain a presence on that platform, you can deactivate the account.

For assistance with this, refer to the help centre on the social media platform.