Note: Delete this page and following pages (total 5 pages) once you complete tailoring the template for your own business

This Policy can be used by all Australian employers and is designed as a guideline intended to provide clarity to employees and contractors on acceptable use of social media platforms when referring to the employer, the employer's products and services, its people, clients, competitors and entities associated with the employer (regardless of whether the devices are owned or controlled by the employer).

The use of social networking sites in the workplace continues to present legal issues. In particular, there has been an increase in cases concerning termination of employment where there is a blurred distinction between work and 'private' activities.

Related documents

- Code of Conduct

Talking points

1. Is posting offensive material on social media grounds for dismissal?

Yes, there have now been a number of cases (and growing) where employers have dismissed employees for their posts on social media.

Example: The Full Bench of (then) Fair Work Australia found that the posting of derogatory, offensive and discriminatory statements or comments about managers or other employees on Facebook might provide a valid reason for termination of employment. In each case, the enquiry will be as to the nature of the comments and statements made and how widely they have been published. Although cases in this area largely turn on their own facts, this decision underscores that a targeted up-to-date and consistently applied policy is critically important when considering disciplinary action against employees for inappropriate use of social media policy and selective application of its disciplinary policy to be particularly relevant. See Linfox Australia Pty Ltd v Stutsel [2012] FWAFB 7097.

2. Is an employer's social media policy able to apply 'beyond work'?

Yes, the Fair Work Commission found that it is legitimate for an employer to establish a social media policy that applies beyond an employee's activities 'at work' in order to protect its reputation and the security of its business.

In this case, the Commission stated: "Gone is the time (if it ever existed) where an employee might claim posts on social media are intended to be for private consumption only…it is difficult to see how a social media policy designed to protect an employer's reputation and security of the business could operate in an 'at work' context only".

The Commission held that the employer had a valid reason for the dismissal given the employee's repeated policy breaches, the evidence that the employer's policies were clear and understood, the employee having been put on notice about the consequences of further breaches and the legitimacy of requesting an employee to acknowledge the employer's social media policy. See Pearson v Linfox Australia Pty Ltd [2014] FWC 446.

Facebook use by employees

Fair Work Australia determined in a matter that "a Facebook posting, while initially undertaken outside working hours, does not stop once work recommences. It remains on Facebook until removed, for anyone with permission to access the site to see… It would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from any consequences.

A Facebook entry could be considered in similar manner to the principle applied under 'out of working hours conduct'. However, it should be noted that the employee's dismissal in this matter was considered to be harsh, unjust or unreasonable. See Fitzgerald v Dianne Smith T/A Escape Hair Design [2010] FWA 7358.

The Fair Work Commission made an order to stop bullying based on repeated unreasonable behaviour over an extended period of time. This behaviour included:

- belittling and humiliating the employee by acting in an aggressive and rude manner
- speaking abruptly to the employee and treating her differently to other employees
- making unreasonable comments to the employee
- acting inappropriately by referring to the employee as 'a naughty little school girl running to the teacher' during a meeting for making a complaint, and
- defriending the employee on Facebook after this meeting.

See Roberts v View Launceston Pty Ltd [2015] FWC 6556.

Getting it wrong

An employer who is in doubt about the correct answer to the question of "Does my workplace need a social media policy?" should know the answer is a definite **"Yes**".

A commonly expressed view, including that of the Fair Work Commission, is the probability of an employee doing something stupid (or at least, of an employee doing something stupid and posting the evidence on social media channels) is inversely proportional to the employee's understanding of the consequences of that action.

Having a social media policy will assist the employer in defending a claim for unfair dismissal if the employee is dismissed for (say) using derogatory remarks about the employer on social media. It will also communicate to employees that such behaviour is not acceptable when it affects the employment relationship.

Example: The Commission reinstated an employee who had been dismissed for material which he posted on Facebook. The Commission noted the employer did not have a social media policy, but relied on its induction training and handbook. The employee wrongly thought the material being posted was private. The original decision was confirmed on appeal to a Full Bench of the Fair Work Commission. *See Linfox Australia Pty Ltd v Stutsel [2012] FWAFB 7097 (3 October 2012).*

General Information

This Policy sets out in detail the business' approach to the use of internet, email, and computer facilities in the workplace, and acceptable conduct on external blogs and sites.

This Policy also allows subscribers to include provisions relating to monitoring (surveillance) of the use of the business' internet, email, and computer facilities.

Please review each aspect of the Policy to ensure it properly represents the business' intended approach.

Purpose

The Policy applies to all users of the business' IT systems.

Provision of facilities

The Policy provides that internet, email, and computers are to be used for legitimate business purposes and 'reasonable personal use'.

The Policy also incorporates use of a personal home computer or personal electronic devices such as iPads, Tablets, Blackberry's, Palm Pilots, PDAs, other handheld electronic devices, smart phones and similar products that are used to access the employer's IT systems, such as email.

Guidelines for use

This section provides an outline to users regarding the business' expectations in relation to internet, email, and computer use, including protection and use of password and login information.

Employers who allow employee's access to their computer may want to ensure employees use passwords and report lost devices such as iPads or Blackberry's if confidential or sensitive information is available on the personal device. This will assist to avoid breaches of confidentiality, unauthorised disclosure of confidential information and use of personal information.

This section also sets out the conduct expected of a user in the event that a user receives an email message which is in breach of the Policy — for example, an email with a pornographic picture attachment.

Prohibited conduct

The Policy is explicit in relation to the activities which are forbidden.

Blocking email or internet access

This section is included to ensure the policy complies with the requirements of the **Workplace Surveillance Act 2005 (NSW) i**n relation to notifying employees if the employee intends to block employees' email or internet access (there are additional obligations in the NSW Act which are covered below). Although the NSW Act only applies in NSW, the business may wish to have a policy which applies nationally. This section should only be deleted if the business does not have operations in NSW.

The Policy reflects an employer's right under the NSW Act to block an email or an internet website if the content of the email or the website is considered to be offensive, illegal, or defamatory.

Access and Storage

The Policy clearly sets out what information is logged and who in the business has rights to access the logs and content of employee email and browsing activity. It also sets out in what circumstances IT staff can legitimately access employee emails and browsing logs.

Monitoring

This clause provides that monitoring of user access is covered by this policy. The clause also clearly states that all use (including personal) of company equipment is monitored and that employees should not expect privacy.

Caution: Employers located **outside New South Wales** should check for any relevant legislative requirements for workplace surveillance in the State or Territory in which they operate. It may be

necessary for these employers to amend the Policy so it complies with the requirements under any other relevant legislation. We advise that any proposed amendments are reviewed by a lawyer.

Breach of the Policy

This clause describes the business' entitlement to take a range of disciplinary actions (including immediate termination of employment) in the event that a user breaches the Policy. Obviously, termination of employment is subject to a number of laws and specific legal advice should be obtained prior to any termination.

The clause also indicates that if an independent contractor to the business has breached the Policy, they may have their contract with the business terminated. Ensure that your contractual arrangements with independent contractors permit termination of the contract in circumstances where there has been a breach of the business' policies. Again, the business should obtain legal advice prior to terminating an independent contractor arrangement on this (or any other) basis.

Blogging facility

This clause outlines employees' obligations to the business when contributing to blogs and websites.

Implementing the Policy

Once the Policy has been finalised, it should be properly implemented to ensure it operates effectively, and to maximise the ability of the business to enforce the Policy. This includes distributing the Policy, conducting initial training sessions to educate users, continuing to inform users about the policy (for example, by use of automatically generated on-screen reminders which 'pop-up' periodically on a user's computer screen), and enforcing the Policy consistently and fairly. New employees should be informed about the Policy and trained in its requirements, preferably prior to commencing employment.

Surveillance of systems

Employers should be aware that the NSW Act prescribes that certain notification requirements must be met before any surveillance of computer systems can be conducted by an employer. A brief description of those requirements is outlined below. Legal advice should be sought in the event of any uncertainty.

Covert and overt surveillance

The **NSW Act** regulates both covert and overt surveillance. An employer can only implement covert surveillance in the workplace if a court grants the employer a covert surveillance authority.

The Policy only deals with overt workplace surveillance. Legal advice should be obtained prior to the business conducting any proposed covert surveillance.

Notification requirements

The **NSW Act** requires an employer to comply with the following notice requirements before commencing overt workplace surveillance:

The affected employee(s) **must be notified in writing at least 14 days** before the surveillance commences. However, the employee(s) may agree to a lesser period of notice.

- The notice must indicate:
- the kind of surveillance to be carried out (ie computer);
- how the surveillance will be carried out;

- when the surveillance will start;
- whether the surveillance will be continuous or intermittent; and
- whether the surveillance will be for a specified limited period or ongoing.

If an employer has already commenced surveillance of employees at work, or is due to commence surveillance less than 14 days after a new employee is due to commence work, the employer need only provide the new employee with the requisite written notice, before the employee starts work with the employer.

There are additional requirements for computer surveillance under the NSW Act. Computer surveillance of employee(s) must not be carried out unless:

- the surveillance is carried out in accordance with a policy of the employer on computer surveillance of employees at work; and
- users have been notified in advance of that policy, in such a way that it is reasonable to assume that they are aware of and understand the Policy.

How to complete this template

Designed to be customised

It is completely customisable based on your specific requirements.

Include what you must and can comply with

This document should be used in conjunction with your contract of employment, and any specific company procedures and processes. Only include the commitments you are confident you can comply with, make sure you update and review the document regularly.

Important: You may have legal obligations to your employees under an employment or industrial agreement such as an award, workplace agreement or employment contract. Make absolutely certain what's written in this document is consistent with these. If you're unsure what covers your employees, ACFA Members can contact ACFA's workplace advice team on 1300 342 248 or on 02 4340 2000 for further advice/assistance.

To complete the template:

1. Using Word's Replace function, search for (INSERT COMPANY NAME) and replace with your company name.

2. Replace (items in brackets) with your own wording.

3. Once you have finished work on the template, delete the first TWO pages of the document.

Disclaimer

As content added includes materials from third parties the Australian Cabinet and Furniture Association (ACFA) does not make any representations or warranties (expressed or implied) as to the accuracy, currency or authenticity of the information. To the full extent permitted by law, ACFA will not be liable or responsible for any third-party materials. The Australian Cabinet and Furniture Association, its employees and agents do not accept any liability to any person for the information in this document.

Internet, Email and Computer Use Policy

1. Purpose

1.1 This Internet, Email and Computer Use Policy ('Policy') sets out the standards of behaviour expected of persons using (insert company name)'s computer facilities, or when making reference to (insert company name) on external sites.

2. Commencement of Policy

2.1 This Policy will commence from XX/XX/XXXX. It replaces all other policies relating to use of (insert company name)'s computers, internet and email facilities (whether written or not).

3. Application of Policy

3.1 This Policy applies to all people who use (insert company name)'s computer network by any means ('***users'***). The Policy also applies to users who contribute to external blogs and sites that identify themselves as associated with (insert company name).

3.2 This Policy does not form part of any employee's contract of employment. Nor does it form part of any other user's contract for service.

4. Definitions

4.1 In this Policy:

a) '***Blogging***' means the act of using web log or 'blog'. 'Blog' is an abbreviated version of 'weblog' which is a term used to describe websites that maintain an ongoing chronicle of information. A blog is a frequently updated website featuring diary-style commentary, audio-visual material and links to articles on other websites.

b) '***Confidential information***' includes but is not limited to trade secrets of (insert company name); non-public information about the business and affairs of (insert company name) such as: pricing information such as internal cost and pricing rates, production scheduling software, special supply information; marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; commission structures; contractual arrangements with third parties; tender policies and arrangements; financial information and data; sales and training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from (insert company name) or obtained in the course of working or providing services to (insert company name) that is by its nature confidential.

c) '***Computer surveillance***' means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of (insert company name)'s computer network (including, but not limited to, the sending and receipt of emails and the accessing of websites).