Social media policy Q&A: Singapore

by Jenny Tsin and Kylie Peh, WongPartnership LLP

Country Q&A | Law stated as at 31-Jan-2021 | Singapore

Singapore-specific information concerning the key legal and commercial issues to be considered when drafting a social media policy for use internationally.

See also *Standard document, Social media policy: International*, with country-specific drafting notes.

Applicability

1. In your jurisdiction, is a policy such as *Standard document, Social media policy: International* usually:

- Put in place by employers?
- Included in a general IT and communications systems policy or as a free-standing policy?

It is useful and fairly common for employers to introduce a social media policy such as *Standard document, Social media policy: International* so that employees have clear boundaries as to the employer's stance on the relevant issues and obligations. However, it is optional and there is no statutory obligation for employers to do so.

Whether the social media policy is included in a general IT and communications systems policy or as a free-standing policy is at the discretion of the employer. There is no difference in terms of legal effect.

2. What are the terms in a policy called in your jurisdiction? For example, clauses, paragraphs, articles.

Typically, the terms in a policy would be referred to as clauses or paragraphs.

3. Does *Standard document, Social media policy: International* help to minimise risk for employers by defining what is acceptable and unacceptable uses of social media in the context of the employment relationship?

Yes, a policy such as *Standard document, Social media policy: International* would help to minimise risks for employers by defining the acceptable and unacceptable uses of social media in the context of the employment relationship. In this context, examples of the risks employers face may include:

- Breaches of confidentiality.
- Breaches in the collection, use or disclosure of personal data.
- Defamation.
- Damage to the employer's reputation.

Adopting a policy can also assist if the employer decides to take disciplinary action against the employee in the event that the policy is breached.

4. Is it possible in your jurisdiction for *Standard document, Social media policy: International* to apply to an employee's social media use, including outside of office hours?

Yes, but that should be explicitly stated. This is especially so where an employee's post on social media refers to their employment relationship with the employer.

Enforceability

5. Is *Standard document, Social media policy: International* enforceable against employees? How?

Yes. *Standard document, Social media policy: International* may be enforced against an employee through:

- An express term of the contract which expressly refers to an employee's obligation to abide by the employer's policies.
- An implied term in the contract that an employee will serve the employer in good faith and fidelity (*Man Financial (S) Pte Ltd (formerly known as ED & F Man International (S) Pte Ltd v Wong Bark Chuan David [2008] 1 SLR(R) 663 at [193]*), which could include an employee's compliance with the employer's policies (including any social media policy) (see *Question 17* and *Question 18*).

6. Can an employer take disciplinary action for breach of the social media policy (as set out in *Standard document, Social media policy: International: clauses 2.3* and *9*)?

Yes, an employer may take disciplinary action for breach of such a policy. It is good practice for the consequences of breach of the social media policy to be stated in either the policy (such as in *clauses 2.3* and *9*) or the employment contract.

7. What disciplinary procedures should the employer follow where the employee is in breach of *Standard document, Social media policy: International*?

The employer should follow the disciplinary procedures set out in its own policy or rules. A failure to do so when such procedures exist can amount to a breach (by the employer) of the employment terms.

If the employer has no disciplinary policy in place, due inquiry should be carried out before disciplinary action is taken.

In determining what constitutes "due inquiry" in the absence of a written policy, the Singapore High Court found in *Long Kim Wing v LTX-Credence Singapore Pte Ltd* that, in the context of an employment contract which provided that "the [c]ompany may after due inquiry dismiss without notice an employee on the grounds of misconduct inconsistent with the fulfilment of the express or implied conditions of his/her service", "due inquiry" would include having a process in place to inform the employee concerned of the allegation(s) and evidence against them, as well as provide an opportunity to defend themselves (*[2017] SGHC 151 at [161]*).

Whether the disciplinary action takes place under an existing policy or not, where there are allegations of misconduct and the employer is intending to take disciplinary action against the employee, it is best practice for the employer to conduct an inquiry before determining the appropriate disciplinary action.

Where the employee is dismissed without notice as a result of disciplinary action, it is not just best practice but mandatory to have held a due inquiry before taking such action (*section 14, Employment Act*).

8. Is the employer required to carry out an investigation before taking any action against an employee in respect of *Standard document, Social media policy: International*?

It is always best practice for an employer to carry out an investigation ("due inquiry") before taking any disciplinary action against an employee, to ensure accountability on the employer's part and increase confidence among employees that there are proper processes and procedures in place.

It is a statutory requirement to conduct a due inquiry before dismissing an employee without notice on grounds of misconduct (see *Question 7*).

9. What disciplinary sanctions may be brought against the employee for breach of the social media policy? Can an employee be dismissed (as set out in *Standard document, Social media policy: International: clause 2.3*)?

The disciplinary sanctions that may be brought against the employee for breach of the policy depend on the disciplinary procedures that have been put in place by the employer. Generally, they may cover the following range:

- Informal discussions.
- Formal warning.
- Suspension.
- Dismissal.

An employee may be dismissed where there has been:

- Gross misconduct (under common law) (*Phosagro Asia Pte Ltd v Piattchanine, Iouri [2016] 5 SLR 1052*).
- Misconduct inconsistent with the fulfilment of the conditions of employment.

The employment contract may specifically define what will constitute gross misconduct. Where the employment contract is silent, the courts have considered the common law principle of repudiation in determining whether there is sufficient misconduct to terminate an employee (*Phosagro Asia Pte Ltd v Piattchanine, Iouri [2016] 5 SLR 1052*). It should be noted that, where an employer is seeking to summarily dismiss an employee, due inquiry must first be conducted (see *Question 7*).

10. Can an employee be required to provide their personal passwords and log in details for social media accounts as set out in *Standard document, Social media policy: International: clause 9.1*?

Organisations may only collect personal data, for example, personal passwords and log in details for social media accounts in accordance with the Personal Data Protection Act (Act No. 26 of 2012) (PDPA), and only for purposes that a reasonable person would consider appropriate in the circumstances.

Under the PDPA, personal data includes "data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access". Therefore, personal passwords and log in details could come under the ambit of personal data.

Under section 13 of the PDPA, an employer may collect, use or disclose personal data where:

- The individual gives, or is deemed to have given, their consent under the PDPA to the collection, use or disclosure.
- The individual has not given consent to collection, use or disclosure, but the collection (or use or disclosure) is required or authorised under the PDPA or any other written law.

In particular, the organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances (*section 18(a), PDPA*). Depending on the context, requiring employees to provide their personal passwords and log in details for their personal social media accounts may not be reasonable or appropriate.

11. Can an employer draw negative inferences about the employee if they do not provide their passwords and log in details when requested to do so by their employer?

If an employee is not co-operative during a disciplinary inquiry, the employer may draw negative inferences against the employee. The employee's non-cooperation would be one of the matters the employer considers in determining whether the employee has breached their obligations to the employer. The employer should also consider the reasons (if any) given by the employee for not providing the passwords and log in details when considering whether negative inferences are warranted.

12. What potential criminal offences could result from the misuse of social media in your jurisdiction?

The misuse of social media may result in a variety of potential criminal offences, depending on the nature of the misuse. The most relevant among them are discussed below.

Protection from Harassment Act

It is a criminal offence under the Protection from Harassment Act (PHA) to cause harassment to another person, via social media or otherwise. It would constitute an offence under the PHA if an employee, with intent to cause harassment, alarm or distress to another person:

- Uses any threatening, abusive or insulting words or behaviour; or
- Makes any threatening, abusive or insulting communication, thereby causing that other person or any other person harassment, alarm or distress.

A similar criminal offence is caused if the employee's actions (as described above):

- Are heard, seen or otherwise perceived by any person likely to be caused harassment, alarm or distress.
- Are made toward a public servant / public service worker in relation to their execution of duty.

In addition, it will also be a criminal offence if the employee's actions (as described above) are done with the intent to:

- Cause the victim to believe that unlawful violence will be used against the victim or any other person.
- Provoke the use of unlawful violence by the victim or another person against any other person.

If the employee uses social media with the intention to unlawfully stalk their victim, causing harassment, alarm or distress to the victim (or they knew or/reasonably should have known that harassment, alarm or distress to the victim is likely), this constitutes a criminal offence.

A person found criminally liable under the PHA is potentially exposed to a range of penalties, ranging from a fine not exceeding SGD5,000 or to imprisonment for a term up to 12 months or to both (depending on the nature of the criminal offence).

Note that applicants under the PHA can also obtain civil remedies against persons who contravene the PHA in certain situations.

Sedition Act

The employee will be in breach of the Sedition Act if they use social media to attempt to:

- Bring into hatred or contempt or excite disaffection against the Singapore government.

- Excite Singapore citizens or residents to attempt to procure in Singapore the alteration, other than by lawful means, of any matter as established by law.
- Bring into hatred or contempt or excite disaffection against the administration of justice.
- Raise discontent or disaffection amongst the citizens or residents of Singapore.
- Promote feelings of ill-will and hostility among different races or classes in Singapore.

The employee will be liable on conviction for a first offence to a fine not exceeding SGD5,000 or to imprisonment for a term not exceeding three years, or to both. For a subsequent offence, the employee will be liable to imprisonment for a term not exceeding five years.

Penal Code

The misuse of social media potentially exposes an employee to liability for a variety of criminal offences under the Penal Code (for example, using social media to deliberately wound the racial or religious feelings of a specific person, or seeking to create enmity between different racial and religious groups).

It is also a criminal offence to intimidate another by threatening to cause any injury to them, their reputation or property, with intent to cause alarm to that person, or to cause that person to do any act which they are not legally bound to do (or omit to do any act which they are legally entitled to do).

If an employee uses social media to make or publish any imputation concerning any person, intending to harm, or knowing or having reason to believe that that imputation will harm, that person's reputation, that will constitute defamation under the Penal Code.

Depending on the act, the employee will be liable on conviction to a range of penalties, from a fine to an imprisonment term to both.

Protection from Online Falsehoods and Manipulation Act 2019

It is a criminal offence, among other things, to do any act in or outside Singapore to communicate in Singapore (via social media or otherwise) a statement knowing or having reason to believe that both:

- It is a false statement of fact.
- The communication of the statement in Singapore is likely to be prejudicial to certain issues of public interest (for example, if that act is likely to be prejudicial to the security of Singapore or if it incites feelings of enmity, hatred or ill-will between different groups of persons).

If guilty, an individual may be fined not more than SGD50,000 or imprisoned for a term not exceeding five years, or both; in any other case (that is, where the offender is not an individual), a fine not exceeding SGD500,000 may be imposed.

Maintenance of Religious Harmony Act

If an employee uses social media to, among other things, incite, instigate or encourage any religious group or religious institution to:

- Cause feelings of enmity, hatred, ill-will or hostility between different religious groups.
- Carry out activities to promote a political cause, or a cause of any political party while, or under the guise of, propagating or practising any religious belief.
- Carry out subversive activities under the guise of propagating or practising any religious belief.
- Exciting disaffection against the President or Singapore government while, or under the guise of, propagating or practising any religious belief.
- If the employee has committed or is attempting to commit any of these acts, the Minister may make a restraining order against them. If the restraining order is breached, they will be liable to a fine not exceeding SGD10,000 or to imprisonment for a term not exceeding two years or to both.

Personal Data Protection Act 2012

Singapore's parliament has recently passed amendments to the PDPA which have not yet come into force. It is not presently clear when these amendments will come into force but it is expected this will take place in early 2021. These amendments will introduce a number of criminal offences under the PDPA which will be relevant.

Under the amended PDPA, an employee will be guilty of an offence punishable upon conviction with a fine of up to SGD5,000 or imprisonment for up to two years or to both, if the employee, without authorisation either:

- Discloses or causes the disclosure of personal data and does so knowing the disclosure is unauthorised or reckless as to whether the disclosure is authorised.
- Uses personal data and does so knowing the use is unauthorised or reckless as to whether the use is uauthorised, and obtains a gain for themselves or another person, causes harm to another individual or causes loss to another person.
- Employers can also be vicariously liable for their employees' social media use (for example, where an employee discloses personal data in breach of the PDPA). In *Executive Coach International Pte Ltd [2017] SGPDPC 3*, the personal data protection commission (PDPC) found that a director of an organisation who had disclosed the past personal history of an individual in a WhatsApp group chat without her consent and without notifying her of the purpose of the disclosure had been acting in the course of his employment and in breach of the PDPA. Accordingly, the organisation was found to have breached the PDPA. Although this matter involve the use of WhatsApp, the PDPC may apply similar principles to cases involving disclosures of personal data on social media.
- Under the amended PDPA. where the PDPC finds that an organisation has intentionally or negligently contravened certain key obligations in the PDPA (for example, to obtain consent for collection, use or disclosure of personal data, not to retain personal data for longer than is necessary and so on) it may impose a financial penalty on an organisation of up to SGD1 million.
- Further, the maximum financial penalty that the PDPC can impose will soon be increased to up to 10% of the annual turnover of the organisation (where the organisation's annual turnover in Singapore exceeds SGD10 million) or up to SGD1 million (in any other case). This revised financial penalty cap will come into effect no earlier than one year after the new amendments to the PDPA come into force.

13.What potential civil claims could be brought against an employee from the misuse of social media in your jurisdiction?

The following potential civil claims could be brought against an employee:

- **Defamation.** While potentially a criminal offence (see *Question 12*), defamation may also attract civil liability under the tort of defamation, codified in the Defamation Act.
- **Harassment.** Civil proceedings in respect of acts of harassment may be brought under the PHA (see also *Question 12*).
- **Data protection.** Persons who have suffered loss or damage as a result of a contravention of certain obligations in the PDPA (for example, to obtain consent for collection, use or disclosure of personal data, not to retain personal data for longer than is necessary and so on) may also bring civil proceedings under the PDPA.

14. Can an employer require an employee to remove any social media content that it considers to constitute a breach of the social media policy (as set out in *Standard document, Social media policy: International: clause 9.2*)?

Yes, the employer may require an employee to remove any social media content which it considers to constitute a breach of *Standard document, Social media policy: International: clause 9.2* or the terms of the employment contract. The employer may also require the employee to remove any social media content if it breaches any applicable laws.

15. Can an employer take disciplinary action if an employee fails to remove any social media content that the employer considered to constitute a breach of the social media policy (as set out in *Standard document, Social media policy: International: clause 9.2*)?

Yes (see also *Question 6*).

Contractual status

16. Is it advisable for the social media policy not to form part of an employee's contract of employment in your jurisdiction so that an employer can make changes as it wishes without breaching the contract of employment with its employees (as set out in *Standard document, Social media policy: International: clause 1.4*)?

Whether to have *Standard document, Social media policy: International* as part of the contract or otherwise is generally up to the employer.

Where the social media policy is not part of the contract, this has the added advantage of flexibility, as its provisions can be more easily amended without the risk of the employer breaching the employment contract.

17. If *Standard document, Social media policy: International* does not form part of the employee's contract of employment, could there be an implied contractual duty on the employee to comply with this policy?

Yes (see *Question 5*).

18. Could an employee be in breach of contract if they are in breach of the social media policy, even where it is stated that the policy does not form part of the employee's contract of employment as set out in *Standard document, Social media policy: International: clause 1.4*?

Yes (see *Question 5*).

19. If *Standard document, Social media policy: International* is non-contractual could this reduce its legal force in your jurisdiction?

The arguments for enforceability would be potentially different.

If the social media policy is part of the contract, its breach can be enforced as a stand-alone obligation.

If the social media policy has not been incorporated into the employee's employment contract, it may still be enforceable against an employee by taking the position that the employee is bound by the implied term of good faith and fidelity to comply with the company's policies, including compliance with the social media policy (see *Question 5*). Alternatively, there may be some other clause (for example, in the clause permitting summary dismissal or in the disciplinary policy) which provides that a breach of the social media policy could give rise to specific consequences.

20. Can the social media policy be amended at any time by an employer in your jurisdiction (as set out in *Standard document, Social media policy: International: clause 1.4*)? If not, what steps should the employer take when it needs to amend this policy?

Standard document, Social media policy: International: clause 1.4 would generally allow the employer to amend the social media policy unilaterally. The employer should inform its employees of the amendments.

Restrictions

21. Can the employer prohibit its employees from the uses of social media as set out in *Standard document, Social media policy: International: clauses 4.1 to 4.4* inclusive?

Yes. This provision does not breach any laws in Singapore.

22. Can an employer prohibit its employees from adding business contacts made during the course of their employment to personal social networking accounts (as set out in the first option in *Standard document, Social media policy: International: clause 4.5*)?

Generally, an employer in Singapore is allowed to dictate its own rules and procedures in relation to social media use; there is no legislation that governs this.

23. Can all the contact details of business contacts made by employees during their employment be the employer's confidential information in your jurisdiction (as set out in the second option of *Standard document, Social media policy: International: clause 4.5*)?

In the employment context, the following categories of information may be protected on account of confidentiality:

- Trade secrets (information that is generally not known outside of the company/employer or reasonably ascertainable by others, and which gives the employer an economic advantage over its competitors and customers).
- Mere confidential information (information which has been communicated to the employee in confidence and with the obligation that the information must be kept confidential).

Generally, business contacts could fall within the category of "mere confidential information". To maintain such confidentiality, employers should:

- Impose clear express confidentiality obligations on their employees through employment agreements.
- Clearly mark the information as "confidential" so that it will have the necessary quality of confidence. *Standard document, Social media policy: International: clause 4.5* expressly provides that the contact details of business contacts made during the course of employment are considered confidential information, and *clause 4.4* provides that the employee must not do anything to jeopardise the employer's trade secrets, confidential information and intellectual property. This would likely be sufficient to impose an obligation of confidentiality on the employee.

24. If not, how can an employer protect against such information being used by employees to compete with the employer or solicit its customers/clients?

An employer may include a confidentiality clause in the employment contract as a measure to protect the employer's confidential information and trade secrets (see *Question 23*).

Alternatively, an employer may insert restrictive covenants into the employment contract, such as non-competition clauses or non-solicitation clauses.

While restrictive covenants are, on the face of it, unenforceable in Singapore, the employer may be able to enforce a restrictive covenant against the employee where:

- It can prove that there is a legitimate proprietary interest protected by the restrictive covenant.
- The restrictive covenant is reasonable in its content and scope.

(*Man Financial (S) Pte Ltd (formerly known as E D & F Man International (S) Pte Ltd) v Wong Bark Chuan David [2008] 1 SLR(R) 663 at [79].*)

Trade secrets and confidential information have been acknowledged as a legitimate proprietary interest (*Clearlab SG Pte Ltd v Thing Chong Chai [2015] 1 SLR 163*).

It should however be noted that having both a confidentiality clause and a restrictive covenant in an employment contract may have an adverse impact on the effectiveness of the restrictive covenant in the contract. In *Stratech Systems Ltd v Nyam Chiu Shim (alias Yan Qiuxin)*, the Singapore Court of Appeal held that the court would not uphold a restrictive covenant where (among other factors), the benefit from having a restrictive covenant (for example, the protection of confidential information) is already protected by another clause in an employment contract such as a confidentiality clause (*[2005] 2 SLR(R) 579*). In such a case, the employer would have to show that the legitimate interest went beyond just the protection of confidential information.

25. Can an employer place an obligation on employees to provide copies of all business contacts and for employees to delete any such information from their personal social networking accounts on termination of their employment (as set out in the second option of *Standard document, Social media policy: International: clause 4.5*)?

Yes, *Standard document, Social media policy: International: clause 4.5* would not contravene Singapore law. An employer may argue that the information belongs to the employer as it was obtained by the employee in a professional capacity, while they were working for the employer, and not in a personal capacity. It is common for termination clauses in employment agreements to provide for all company property (including personal and proprietary information) to be returned to the employer on termination.

26. If an employee is required to speak on behalf of the employer, can the employer impose certain requirements and restrictions on the employee as referred to in *Standard document, Social media policy: International: clause 5.1*?

Yes.

27. When an employee discloses an affiliation with their employer on their personal social media, can an employer include provision in the policy for the employee to state that their views do not represent the views of the employer as set out in *Standard document, Social media policy: International: clause 6.3*?

Yes.

28. Can an employer include provision in the policy for an employee to refrain from posting anything until the employee has discussed it with their manager (as set out in *Standard document, Social media policy: International: clause 6.4*)?

Yes.

Monitoring

29. In your jurisdiction, can internet postings and social media use by employees be monitored by employers?

Where employees' postings and social media use are publicly available, employers are allowed to view and monitor them. Conversely, if such postings are private, then the employer may only monitor them where the collection, use and disclosure of personal data is in line with the PDPA, and only for purposes that a reasonable person would consider appropriate in the circumstances (see *Question 30*).

Depending on the facts, the employer may monitor internet postings and social media use by employees which are made using the employer's devices or network resources (such as office computers or mobile devices) with the employee's consent or if the employer can demonstrate that the collection, use and disclosure of the personal data falls within the scope of one of the statutory exceptions under the PDPA. In particular, the PDPA provides that the employer can use, collect or disclose the personal data without the consent of its employees for the purpose of managing its employment relationships. This includes monitoring how the employee uses the employer's computer network resources (*paragraph 5.21, Personal Data Protection Commission Advisory Guidelines on the PDPA for Selected Topics*) (PDPA Guidelines). However, section 20(4) of the PDPA provides that even though consent is not required, the employer is nevertheless required to notify the employees of the purposes of the collection, use or disclosure of personal data.

30. On what basis can an employer legally monitor its employees' social media use?

An employer may legally monitor its employees' social media use on the employer's devices where the employer has obtained the employee's consent for the collection, use or disclosure of their personal data against notified purposes, which must be purposes that a reasonable person would consider appropriate in the circumstances. Otherwise, the employer must show that the collection, use and disclosure of the personal data falls within the scope of one of the statutory exceptions under the PDPA (for example, for the purpose of managing or terminating an employment relationship between the employer and the employee (*paragraph 5.21, PDPA Guidelines*)). Monitoring internet usage could likely fall under the ambit of managing its employment relationship.

Employers should note that although consent is not required from their employees to collect, use or disclose their personal data for the purposes of managing the employment relationship if the employer seeks to rely on the statutory exception as discussed above, employers must still notify their employees of the purposes of the collection, use or disclosure (*section 20(4), PDPA; paragraph 5.19, PDPA Guidelines*).

In relation to employees' social media use on their own devices, an employer may legally monitor use if the information and postings are publicly available (that is, there are no specific rules prohibiting employer monitoring when the information and postings are available for everyone's viewing in the public domain). Conversely, where employees' social media use is on their own devices and where the information and postings are private, employer monitoring is only allowed if the employees have expressly consented to these purposes that a reasonable person would consider appropriate in the circumstances (*sections 14 and 18(a), PDPA*).

31. Can an employer monitor employees using the employer's IT resources and communications systems to ensure that its rules and policies are being complied with and for legitimate business purposes as set out in *Standard document, Social media policy: International: clause 7.1*?

Yes (see *Question 30*). An employer may only monitor employees where the collection, use and disclosure of personal data is in line with the PDPA. Given that these practices can be intrusive, employers may wish to expressly obtain the employee's consent for the collection, use or disclosure of their personal data for such monitoring, which must be for purposes that a reasonable person would consider appropriate in the circumstances.

Otherwise, the employer may only monitor employees without consent if the employer can show that the collection, use and disclosure of the personal data falls within the scope of one of the statutory exceptions under the PDPA (for example, for the purpose of managing or terminating an employment relationship between the employer and the employee). If relying on such an exception, the employer must comply with any statutory requirements for the relevant exception, which could include notifying the employees of the use, collection or disclosure and the purpose of doing so.

Employers also must be aware of the implied mutual duty of trust and confidence between them and their employees (*Wee Kim San Lawrence Bernard v Robinson & Co (Singapore) Pte Ltd [2014] SGCA 43*), and not breach this by abusing their ability to monitor.

32. Are there any legal requirements or limitations that an employer needs to be aware of when monitoring its employees' social media use in your jurisdiction?

An employer must ensure that its actions comply with the PDPA. In particular, employers may wish to seek their employee's consent for the collection, use or disclosure of personal data for such monitoring. Otherwise employers should ensure the collection, use or disclosure falls within the scope of one of the statutory exceptions and comply with any statutory requirements for such exceptions (see *Question 31*).

An employer must also ensure that the purpose, scope and extent of the monitoring is reasonable and in line with the implied term of trust and confidence that it has with its employees (see *Question 31*).

33. If consent is required for such monitoring, is the consent provided by the employee in *Standard document, Social media policy: International: clause 7.1* sufficient?

Where the employee signs the social media policy and returns it to the employer, this would be deemed valid consent. *Clause 7.1* appears to be sufficient to allow the employer to monitor the employee's social media activities for the purposes of compliance and for legitimate business purposes. However, to protect the employer's position better and to ensure that the employer is able to monitor social activities for compliance with the law, we would suggest the following amendments:

"We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our

rules are being complied with, and for legitimate business purposes and for compliance with any and all applicable laws, and you fully consent to such monitoring by your use of such resources and systems."

Recruitment

34. In the recruitment process, can employers use internet searches to perform due diligence on candidates as set out in *Standard document, Social media policy: International: clause 8*?

Yes. Where the information on an individual is publicly available, organisations are not required to seek consent from the individual (*paragraph 5.3, PDPA Guidelines*).

35. Can a recruiting employer lawfully rely on information gained from a prospective employee's available social media activity?

Yes, a recruiting employer may lawfully rely on information gained from a prospective employee's available social media activity. However, employers should be cautious to rely solely on this public information, and should, if possible, as a matter of best practice, try to verify independently that the public information is accurate.

Employers should also be cautious not to allow discriminatory reasons to guide their recruitment decisions. For example, an employer should not decide against hiring a person based on the person's age, religion or other protected characteristic gleaned from social media posts. In this regard, employers may take guidance from the *Tripartite Guidelines on Fair Employment Practices* (the Tripartite Guidelines), which provide, among other things, that the employer should recruit and select employees on the basis of merit (such as skills, experience or ability to perform the job), and regardless of:

- Age.
- Gender.
- Religion.
- Marital status and family responsibilities.
- Disability.

36. Is there a risk that an unsuccessful job applicant could claim discrimination where an employer has accessed their available social media activity during the recruitment process?

Yes. If an employer relied on the information available through the job applicant's social media to make its decision, and reliance on this public information could be construed to be discriminatory, the unsuccessful job applicant could raise a complaint of discrimination with the Ministry of Manpower (MOM). When this happens, the MOM will investigate and the employer will be given an opportunity to present its case. If the complaint is substantiated and the employer has contravened the Tripartite Guidelines, the employer will generally be given the opportunity to rectify its actions. MOM will also inform employers that non-rectification and future occurrences could result in administrative action, including curtailment of work pass privileges (that is, not approving future work pass applications and/or renewals for Singapore employers to employ/continue employing foreign workers).

As a result, an employer should seek to keep proper records documenting the recruitment process, to support the employer's position that its decision to reject the applicant was based on fair and legitimate reasons, and not discriminatory.

37. Can an employer prevent its staff from providing references for other staff on social media and professional networking sites (as set out in *Standard document, Social media policy: International: clause 2.2*)?

Yes.

Employee's rights

38. What rights do employees have in your jurisdiction in relation to their personal social media use during employment, for example, a right to privacy, a right to freedom of expression?

There is no legislation providing a general right to privacy. The PDPA is the relevant statute governing the collection, use and disclosure of personal data by organisations (including employers) in a manner that recognises both:

- The right of individuals (including employees) to protect their personal data.
- The need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

(*Section 3, PDPA*.)

As the use of social media involves personal data, the PDPA would apply.

While there is a constitutional right afforded to Singapore citizens to freedom of speech and expression (*Article 14, Singapore Constitution*), this right is subject to several restrictions, including a prohibition on speech that constitutes defamation or incitement to any offence (see *Question 12*).

An employee's right (along with the extent of that right) to personal social media use during employment is largely dependent on the terms of their employment. For example, certain organisations may permit personal social media use during working hours and/or using the organisation's devices, so long as it does not involve professional or inappropriate content, and does not interfere with the employee's employment responsibilities or productivity. Conversely, other organisations may not permit personal social media use during working hours at all. Employers can also restrict use of social media sites on devices provided by the employer.

Outside working hours, employees should be free to use their personal social media.

39. What claims could an employee bring against an employer for breach of such rights?

If an employee's rights under the PDPA have been breached, the employee may make a complaint to the PDPC. For example, an employee may file a complaint if they discover that their internet activity or social media use is being tracked by their employer without having been notified (see *Question 33*). In addition, an aggrieved employee may also have a private right of action against the organisation for relief in civil proceedings in a court.

The PDPC may resolve the situation in a number of ways:

- Assisting in resolving the issue between the employee and organisation.
- Where attempts at resolution fail, the PDPC may refer the matter to mediation, if both parties are agreeable. If the matter is resolved amicably, no further investigations need to be conducted.
- Pursuant to amendments to the PDPA, the PDPC may without the consent of the employee and the organisation, refer the matter to mediation under a dispute resolution scheme, if the PDPC is of the opinion that any complaint by the aggrieved employee may more appropriately be resolved by mediation.

In certain circumstances, the PDPC may exercise its power to review. On the application of a complainant, the PDPC may review:

- A refusal to provide access to personal data requested by the complainant, or failure to do so within a reasonable time.
- A fee required from the complainant by an organisation in relation to a request by the complainant to access or correct personal data.
- A refusal to correct personal data in accordance with a request by the complainant, or failure to make the correction within a reasonable time.

Alternatively, the PDPC may, if satisfied that an organisation is not complying with certain key obligations of the PDPA, give the organisation any directions as it thinks fit in the circumstances to ensure compliance, including an order to:

- Stop collecting, using or disclosing personal data in contravention of the PDPA.
- Destroy personal data collected in contravention of the PDPA.
- Comply with any direction of the PDPC.
- Pay a financial penalty not exceeding SGD1million, as the PDPC deems fit.
- The maximum financial penalty that the PDPC can impose will soon be revised (see *Question 12*).

40. Do the laws in your jurisdiction address potential harassment or bullying between employees via personal social media?

There is no legislation which specifically addresses harassment or bullying via personal social media between employees.

However, the PHA would be the appropriate and primary legislation to address incidents of harassment or bullying, regardless of the medium through which it is conducted (see *Question 12*).

41. What obligations would be placed on employers where there is harassment or bullying between employees via personal social media?

There is no specific statutory obligation for an employer to take action where there is harassment or bullying between employees via personal social media. However, the employer may still be under certain obligations to ensure that the harassment or bullying do not occur in the workplace. The duty to prevent and/or take action in relation to harassment or bullying may be caught by the Workplace Safety and Health Act, which provides that every employer

must take, so far as is reasonably practicable, any necessary measures to ensure the safety and health of its employees at work (although this issue has not been determined by the Singapore courts).

Commentary and case law has suggested that an employer may be deemed negligent if it has no appropriate workplace policies, or may be liable for breach of contract (in particular, breach of the implied term of trust and confidence with their employees) in cases of harassment or bullying (*Ravi Chandran, Workplace Harassment, Persons Liable and Damages Payable under the Protection from Harassment Act 2014 (2015 27 SAcLJ) at [14]*; *Swan v Monash Law Book Co-operative (2013) VSC 326* (although the latter is not a Singapore case, it has been cited in approval in Singapore commentary and would generally be persuasive to the Singapore courts)).

The *Tripartite Advisory on Managing Workplace Harassment*, from which employers in Singapore take guidance as a matter of best practice, recommends that employers take certain steps to ensure a safe workplace. This includes:

- Developing a harassment prevention policy.
- Providing information and training on workplace harassment.
- Implementing reporting and response procedures.

It is highly recommended that any Singapore employer adhere to the Tripartite Advisory on Managing Workplace Harassment.

42. How do these obligations differ where the harassment or bullying is being conducted via personal social media or do the same obligations apply to employers regardless of the bullying or harassment taking place via personal social media or in person?

From a legal perspective, there is no difference between harassment or bullying being conducted via personal social media or in person.

43. Can an employer be vicariously liable for bullying and harassment between employees via personal social media in your jurisdiction?

It is unclear whether the PHA provides for statutory vicarious liability of the employer for acts of bullying or harassment by employees. Presently, there is no case law on the PHA's ambit in this regard, and academic commentaries have suggested that it does not, because:

- Section 11 of the PHA provides that civil proceedings may be brought "against the respondent"; in comparison, other similar statutes (such as section 10 of the UK's Protection from Harassment Act 1997) have specific references to claims being allowed to be made against an employer. Given the lack of a similar

section in the PHA, commentaries have argued that the statute impliedly prohibits vicarious liability for bullying or harassment on the employer's part.

- The Singapore parliament, in passing the PHA, focused on the various possibilities available under the statutory scheme (including mandatory treatment orders, self-help and mediation) without having to resort to civil action. Therefore, commentaries have opined that allowing vicarious liability would shift the focus towards civil claims and compensation, contrary to parliament's supposed intent.

However, English case law (which has high persuasive value but is not legally binding in Singapore) has suggested that an employer may be found to be vicariously liable outside the ambit of statute, especially if the employer is negligent (*Waters v Commissioner of Police of the Metropolis [2000] 1 WLR 1607*). In this regard, case law has suggested that a wronged employee may have a valid cause of action against the employer if the employer fails to protect the employee against victimisation and harassment, although the liability would only be likely to arise if the employer knows or ought to know that victimisation or harassment is taking place and fails to take reasonable steps to prevent it (*Waters v Commissioner of Police of the Metropolis; Helen Green v DB Group Services (UK) Ltd [2006] IRLR 764*).

(The issues above have yet to be determined by the Singapore courts. However, the English cases discussed here have been cited in approval in Singaporean commentary and other cases.)

Reasonable steps could include matters such as:

- Providing counselling.
- Issuing a warning or disciplinary action.
- Transferring the offender to another location or department.

Failing to carry out investigations, or carrying out improper or inadequate investigations, may also result in liability.

Whether an employer is eventually found to be vicariously liable is heavily fact-specific and largely dependent on a variety of factors, such as:

- The relationship between the employer and employee.
- The nature of the harassment or bullying.
- The steps that either party may have taken.

Execution and other formalities

44. Are there any formalities or language requirements that must be adhered to in relation to the creation, introduction or execution of *Standard document, Social media policy: International*?

Formalities

When the social media policy is introduced, to have contractual force it must receive the agreement of the employees. As with any contract, the elements of offer, acceptance and consideration must be present.

As it may not be practicable to require all employees to sign to signify their agreement, employers may seek to obtain consent from their employees by circulating the social media policy and obtaining their acknowledgement of it. This can be done through an electronic platform, such as on the employer's intranet, or simply responding to the email accepting the terms of the social media policy.

If the social media policy is not meant to have contractual force, it should nonetheless be disseminated and brought to the attention of all employees when it is introduced.

From a practical and operational perspective, the employer should also ensure that the social media policy is readily available and easily accessible to its employees.

Language requirements

There are no formal language requirements that must be adhered to in relation to the creation, introduction or execution of the social media policy. However, it would be good practice to provide the terms in a language that the employees understand.

45. Under what circumstances is consultation with or approval of a works council or trade union required for the social media policy (as set out in *Standard document, Social media policy: International: clause 1.3*)?

This depends on the terms of the particular collective agreement. In our experience, collective agreements in Singapore do not usually contain a specific term requiring consultation with or approval of the unions before implementing a social media policy.

Even when it is not required under the terms of the collective agreement, the advantage to the employer of consulting the union is that it would have the union's assent to the social media policy, which reduces the possibility of the union then arguing against its terms in the future. The union could also assist the company in explaining the terms of the social media policy to employees who have breached the terms of such policy.

General

46. Are any of the parts of *Standard document, Social media policy: International* not legally valid and enforceable or not standard practice in your jurisdiction?

No.

47. Are there any other standard clauses that would be usual to see in a social media policy such as *Standard document, Social media policy: International* and/or that are standard practice to include in your jurisdiction?

There are no further clauses which should be included as standard practice.

Contributor details

Jenny Tsin, Partner

WongPartnership LLP
T +65 64168110
E *jenny.tsin@wongpartnership.com*

Areas of Practice: Employment.

Kylie Peh, Partner

WongPartnership LLP
T +65 64168259
E *kylie.peh@wongpartnership.com*

Areas of Practice: Privacy and Data Protection.

END OF DOCUMENT