

IT and Social Media Policies (United Arab Emirates)

by *Charles Laubach* (partner) and *Stephanie Nazareth* (associate), *Afridi & Angell*

Practice note: overview | Law stated as at 01-Feb-2024 | United Arab Emirates

A Note providing an overview of all the key issues to consider when putting in place IT and social media policies in the UAE, some practical guidance for drafting and reviewing the policies.

It also considers the restrictions that an employer can place on employees in respect of their personal use and also any limitations on the employer's ability to monitor their employees.

Introduction

Applicability

- Formalities

- Language requirements

Responsibility

Enforceability

- Disciplinary Action

- Disciplinary Sanctions

- Criminal Offences

- Civil Claims

Contractual Status

Restrictions on Personal Use

IT Security

Social Media

- Employee's Rights

- Harassment and Bullying

- Business contacts

- Recruitment

- References

Monitoring

- Legal Requirements

- Automated Software

- Investigations

- CCTV

ChatGPT

Employers are keen to minimize any risks employees may pose to an organization through their use of IT and social media. This Note considers the rules and practice governing IT and social media policies in the UAE. It sets out the key issues relating to IT and social media policies, and the legal restrictions imposed on employer's monitoring employee use of their systems.

The guidance in this Note is generally applicable throughout the UAE and the free zones. The only exceptions are the Abu Dhabi Global Market (ADGM) and Dubai International Financial Centre (DIFC) free zones, which take a different approach to the application of, for example, onshore privacy law.

Introduction

Employers should be aware that the UAE is a socially conservative jurisdiction and therefore the level of tolerance of certain actions is relatively low. While there is no statutory legislation on what is permissible or not in IT and social media policies, it is advisable that employers avoid making affirmative statements or endorsing their political or ideological leanings. While it is permissible to instruct employees on what should not be done or what is not acceptable in the workplace, employers should avoid statements that require employees, for example, to support or undertake a specific action (for example LGBTQ rights, right to protest, and so on).

Applicability

IT and social media policies are usually put in place by employers. The social media policy is normally included as a free-standing policy.

As long as the employer ensures that the social media policy forms part of the employee's employment contract (see [Enforceability](#)), it can apply to an employee's social media use outside office hours. For example, the employer can impose restrictions if:

- The employer's assets are used (such as the employer's server, wifi connection, or handheld device) in the communication.
- The communication involves the public image of an employee who is public-facing.
- The employer is the sponsor of the employee's visa in the UAE, and so can legitimately require (within reason) that the employee abide by employer rules at all times.

The employer has the right to dictate how an employee uses:

- Hardware provided by the employer (such as laptops and handheld devices).
- The employer's server, email account or similar.
- Any communications that identify the employer (such as communications on employer letterhead or showing the employer's name in a signature block).

The employer also has the right to require that the employee does not engage in any activity during working hours that is not work-related.

To impose any restrictions on private communications made by the employee in the employee's spare time which do not fall into the above categories, the employer must clearly state these in the policy, and the policy must be incorporated by reference into the employment contract (see *Enforceability*). Employers would generally consider this kind of restriction only for an employee whose role is particularly public-facing.

Terms in a policy are generally called clauses.

The IT and social media policies can apply to any person who is subject to the Labour Law and/or has entered into an agreement with the employer to be bound by the employer's terms and conditions.

As such, the policies can also apply to independent contractors, part-time workers, clients, customers, or suppliers of the employer.

Formalities

Employees will need to provide their written consent to be bound by the IT and social media policies, and renewed written consent should be obtained each time the IT social media policies are amended.

This can be achieved by the employee's dated signature on the policies; there are no further formalities required.

Works council or trade unions do not exist in the UAE so no consultation is required in relation to these policies.

Language requirements

There are no language requirements for the employer's IT and social media policies. Global companies do not require to have their policies in Arabic. The policies can be written in English, and the English language is sufficient and acceptable.

However, if any documents must be submitted to the onshore courts for any reason, those documents will have to be translated and certified in Arabic.

Responsibility

It is advisable that the IT and social media policies include details of the personnel responsible for the policy so that in the case of feedback requests or grievances, the employee can approach the relevant officers.

In the UAE, it is standard practice and permissible for managers to have specific responsibility for ensuring the fair application of the IT and social media policies.

Enforceability

UAE labour law permits an employer to have necessary policies in place for an employee to follow. The IT and social media policies will need to form part of the employee's employment contract (or be incorporated into it by reference) in order for the employer to be able to sanction the employee for any breach of the policy.

To be incorporated into the employment contract, the policies must be referred to in the employee's contract of employment and also annexed to the contract, so that the employee consents in writing to being bound by the policies.

Any amendments to the IT and social media policies from time to time will require the employee's written consent to be enforceable against the employee.

Excessive personal use or misuse of the employer's IT and communication systems by an employee can be regarded as misconduct if there was a provision sanctioning this behavior in the IT and social media policies, and the policy formed part of the employee's employment contract.

Disciplinary Action

Depending on the severity of the breach and provided that there is a nexus of damage to the employer, the employer can take disciplinary action against the employee for breach of the IT and social media policies.

It is standard practice for employers to have written disciplinary process and procedures in place and the Labour Law also requires employers to have a list of penalties clarifying each of the disciplinary actions applicable to an employee.

Article 44 of Federal Decree-Law No. 33 of 2021 (Labour Law) expressly provides that if any mistake committed by an employee has resulted in a serious material loss to the employer, the employer is permitted to terminate the employment immediately without notice. Similarly, under the Labour Law, the employee can be terminated immediately without notice if the employee has breached their duties under the employment contract and continues to be in breach despite the employer conducting a written investigation and providing two warnings to the employee regarding the breach. In practice, however, termination of employment under Article 44 of the Labour Law requires that the employer make a compelling case that termination without notice is justified.

Article 41 of the Labour Law expressly provides that disciplinary penalties cannot be imposed on an employee who has committed an act (not restricted to a civil or criminal offence) outside the workplace unless it is work related. Accordingly, the employer must prove that the employee's online actions have had an impact on its business for the employer to take disciplinary action.

For any disciplinary penalties imposed on an employee, it is mandatory for the employer to carry out an investigation to establish the nature of the breach and to ensure that it has a defensible position for any action it may take against the employee (see [Disciplinary Sanctions](#)).

An employer can include provision in its policies requiring employees to provide their personal passwords and log in details for social media accounts, as long as the employee's consent to this being included in the policies. Even so, such action should be approached very cautiously (see [Monitoring](#)). If the provision of passwords and log-in details is a requirement of a policy, and the employee has consented in writing to be bound by that policy, the employer will be entitled to treat any refusal of the request as a breach of the social media policy.

Disciplinary Sanctions

If the employee is found to be in breach, the employer may impose disciplinary sanctions only after giving written notice to the employee, investigating the employee's conduct and hearing the employee's statement in their defence. When applying the disciplinary sanction, the employer must:

- Explain the nature of the breach of the IT and social media policies.
- Give details of the penalty imposed.

- Advise the employee of possible ramifications of future breaches.

Under the Labour Law, disciplinary action must be imposed by an employer after taking into account the gravity and seriousness of the offence. The employer must bear in mind factors such as the extent of breach of confidentiality of work-related data and information, any financial and reputational impact caused by the breach, and the recurrence of the breach committed by the employee.

The Labour Law expressly states that an employer may not accuse an employee of a breach that was detected more than 30 days previously, and may not impose disciplinary sanctions on an employee after more than 60 days from the date of completing an investigation of the breach.

If the breach persists, the employer may then choose to take stricter disciplinary procedures such as suspension of employment, and, if the conduct warrants it, termination. An employer may deduct pay from the employee as a disciplinary action so long as the deduction does not exceed the equivalent of five days' pay per month (Article 39, Labour Law).

An employee can be dismissed by written notice of no less than 30 days for a "legitimate reason" (Article 43, Labour Law). The authors believe that breach of an employer's IT and social media policies, especially when those policies are incorporated by reference into the employment contract, would generally constitute a "legitimate reason" for dismissal (though the existence of a legitimate reason is a finding of fact in each specific case).

Even if dismissal were found to be wrongful, the employee's maximum recovery in damages would be capped at three months' salary (Article 47, Labour Law).

A "severe" breach would justify immediate termination only if it rose to the level of misconduct contemplated by Article 44 of the Labour Law, which is a very difficult standard to meet (though this could possibly be the case if the breach in question constituted a criminal offence as well as a breach of the policy). As noted above, termination of employment under Article 44 of the Labour Law requires that the employer make a compelling case that termination without notice is justified (see [Disciplinary Action](#)).

Having IT and social media policies in place does help to minimise risk for employers by defining what are acceptable and unacceptable uses of the employer's IT and social media in the context of the employment relationship; it also informs employees of the policies and of their obligation to comply with them.

Criminal Offences

The potential criminal offences that could result from misuse of social media and the employer's IT systems include the following:

- Making public another individual or entity's confidential information (Article 432, Federal Decree-Law No 31 of 2021 (UAE Penal Code). This could lead to punishments including temporary imprisonment or a fine.
- Posting defamatory statements or publishing information that exposes another person or entity to contempt or public humiliation on social media platforms (Article 425, UAE Penal Code).
- Taking a picture, publishing, or displaying an image of someone without their active consent (knowledge and failure to object are not sufficient); this would be an invasion of someone's privacy under the Cyber Crimes Law (Federal Decree-Law No.34 of 2021). Additionally, the UAE Penal Code makes it an offence to publish someone's photograph without their prior consent. The Copyright Law (Federal Decree-Law No.38 of 2021) also makes it a crime to publish

or distribute a picture without someone's consent, unless there is an agreement between the two that dispenses with the requirement for consent.

- Mocking the representatives of the UAE, encouraging sinful activity (for example, anything relating to sex, overt displays of affection, or scanty clothing), or making lewd remarks against religion or remarks aimed at corrupting minors (Articles 414-424, UAE Penal Code). These crimes may be punishable by detention for up to six months and a fine of up to AED5,000.

The Cyber Crimes Law provides that the employer can be jointly held liable for fines or other remedies such as confiscation of the hardware or software used in the commission of the offence, or blocking the offending website, if an offence is committed by an employee in the name or on behalf of the employer.

Breaches of the Cyber Crimes Law are punishable by either or both:

- Imprisonment for a period not less than one year.
- A fine not less than AED250,000 and not more than AED1 million.

Civil Claims

The employer can initiate civil proceedings for damages under the UAE Civil Code (Federal Law No. 5 of 1985) where it:

- Has documentary evidence to demonstrate that there has been a disclosure of confidential information or trade secrets.
- Is able to quantify the damage sustained by the business as a result.

It could also bring a separate action for defamation if the employee's use of social media defames the employer or its business.

Civil action could also be taken against the employee by any third parties harmed by the employee's conduct.

In addition to all relevant criminal offences (see *Criminal Offences*), if an employee's misuse of the employer's IT systems (including misuse of email to send an incorrect, improper, or inappropriate content) has caused harm to a third party, a civil claim in tort could be brought against that employee.

The UAE courts, similar to courts in other civil law jurisdictions, do not readily grant injunctive relief or specific performance as a remedy. The UAE Civil Code recognises damages as an appropriate remedy for any civil claims.

An employer can be held vicariously liable for the acts of its employee if a civil claim arises against the employee. For the employer to be liable it will need to be proven that both:

- The employer has power or control over the employee.
- The harmful acts were committed by the employee in the course of their employment.

Contractual Status

The IT and social media policies should form part of the employee's contract of employment, so that they are enforceable against the employee (see *Enforceability*).

If the IT and social media policies do not form part of the employment contract, or if they are not incorporated by reference, then the employee would have to otherwise agree in writing to be bound by the IT and social media policies for them to be enforceable against them. There is no implied contractual duty on the part of the employee to comply with the policies.

However, an employer might be able to take action in some cases even aside from its IT and social media policies. For example, if an employee engaged in a communication that constituted an act contrary to public morals, then the employer might be able to proceed with termination without notice under Article 44(6) of the Labour Law (see *Disciplinary Action*).

Restrictions on Personal Use

An employer can include provisions in its IT and social media policies disallowing employees to access their personal email or other social networking sites during office hours.

It can also include provisions in its policies prohibiting its employees from the following uses of social media:

- Making any social media communications that could damage the employer's business interests or reputation, even indirectly.
- Using social media to:
 - defame or disparage the employer, their staff, or any third party;
 - harass, bully, or unlawfully discriminate against staff or third parties;
 - make false or misleading statements; or
 - impersonate colleagues or third parties.
- Expressing opinions on behalf of the employer via social media, unless expressly authorised to do so by the employee's manager.
- Posting comments about sensitive business-related topics, such as business performance, or do anything to jeopardise the employer's trade secrets, confidential information, and intellectual property.

Including the employer's logos or other trademarks in any social media posting or in the employee's profile on any social media.

When an employee discloses an affiliation with their employer on their personal social media, an employer can include provision in the policy for the employee to state that their views do not represent the views of the employer.

An employer can include a provision in the policy for an employee to refrain from posting anything until the employee has discussed it with their manager. It can also include provisions requiring employees' personal emails sent from the employee's IT systems to be labelled as "personal" in the subject header. Employers can withdraw permission for personal use of their IT systems by employees as employers have the discretion to change their policies at any time. However, as stated above, any amendments to the IT and social media policies will require the employee's written consent to be enforceable against the employee and even if the IT and social media policies do not form part of the employment contract, it is advisable that any changes are notified to and agreed in writing by the employees to be enforceable (see *Enforceability*).

It is standard practice for an employer to restrict or prevent access (including restricting access due to excessive use) to certain internet sites used by an employee.

An employer can require an employee to remove a social media post that it considers to be in breach of the social media policy (if the employee consented in writing to be bound by the policy). The employer may consider taking the disciplinary action for the failure of an employee to remove any social media content that the employer considered to constitute a breach of the social media policy (see *Enforceability* and *Disciplinary Action*).

IT Security

In the UAE, it is permissible for an employer to make employees responsible for the security of both:

- The equipment allocated to and used by them.
- The computer terminal used by them.

Provisions to this effect can be included in the employer's IT and social media policies.

It is also permissible for employers to delete, block access to, or not transmit emails or attachments in the interests of security, and to block access to employees' web-based personal emails such as gmail or Hotmail on the employer's computer system for security reasons.

If the employees are using the employer's IT equipment outside of work, it is common practice for employers to install necessary software and require employees to take necessary precautions to protect against importing viruses and compromising system security in the employer's IT system.

Social Media

The social networking sites typically available and used in the UAE are:

- LinkedIn.
- Facebook.
- Twitter.
- YouTube.
- Google+.
- Instagram.
- SnapChat.
- Pinterest
- Zoom.

Employee's Rights

The Constitution of the UAE contains a general right to privacy for individuals, and guarantees freedom of communication by post, telegraph, or other means of communication. All natural persons have the right to privacy. When that right is surrendered, it must be clear that the person intends to give up this right, and the resulting surrender of privacy will be construed narrowly and not broadly.

It is a crime for a person to use the following to violate the privacy of a person (except in cases permitted by the UAE Cyber Crimes Law):

- An information network.
- An electronic information system.
- Any information technology.

(Article 44, UAE Cyber Crimes Law.)

Violations of these privacy provisions can occur in the following ways, for example:

- Overhearing, intercepting, recording, transferring, transmitting, or disclosing conversations, communications, or audio or visual materials.
- Capturing pictures of a third party or preparing electronic pictures or transferring, exposing, copying, or keeping those pictures.
- Publishing electronic news or pictures or photographs, scenes, comments, statements, or information, even if they were correct and real.

An employee can bring a complaint against their employer for a breach of the Cyber Crimes Law. The employee would have to allege that the employer's conduct constituted a breach of this statute such as, for example, unauthorised disclosure of information, or unauthorised monitoring of communications (see *Monitoring*).

It should be noted that this would not be a claim by the employee for a grievance under the Labour Law, but instead a report of prohibited activity under the Cyber Crimes Law. It might result in the imposition of sanctions on the employer, but it would not result in a remedy for the employee under the Labour Law (see also *Criminal Offences*).

Harassment and Bullying

There is no free-standing anti-harassment law in the UAE (whether relating to online or offline behaviour), but there are a number of legal provisions which may be triggered in the context of workplace harassment, discrimination, and/or bullying.

Bullying and harassment could have arise in one of two ways.

- they could constitute a breach of the employer's own obligations under Article 4 of the Labour Law, under which it is prohibited to "discriminate on the basis of race, colour, sex, religion, national origin, social origin or because of disability, which would impair equal opportunities or prejudice equality in obtaining or continuing a job and enjoying the rights".

Therefore, an employer could be found in breach of its obligations under the Labour Law if the workplace environment was found to be discriminatory.

- They could be found contrary to the prohibitions that appear in the:
 - Penal Code. For example, if a male employee made improperly sexual or intimate remarks about a female employee;
 - Anti-Discrimination Law (Federal Decree-Law No. 2 of 2015). For example, if a colleague made jokes about another colleague's religious beliefs; or
 - Cyber Crimes Law. For example, if a colleague sent a photograph of another colleague to his friends without her consent.

An employer (or its managers) may be liable for the acts of its employees towards another. However, these breaches of law by individuals would only constitute a breach of the Labour Law if the employer was aware of them (or should have been) and did nothing; in that case, the employee would also have grounds for a complaint against the employer, under Article 4 of the Labour Law (see above), which the authorities may be expected to take quite seriously.

Similarly, an obligation will only exist on the employer with regards to harassment or bullying between employees on personal social media where the employer knew or should have known of such conduct.

Under the UAE Anti-Discrimination Law, a "representative, director or agent" of a company could be found liable if an employee commits an offence of discrimination while acting in the company's name or interest. Under the Penal Code, the company itself can be held criminally liable for acts committed by its "representatives, directors or agents" acting on its behalf.

In the event of a dispute, an employer will be required to show that an employee was not acting in the company's name or on its behalf when making discriminatory or harassing comments. Having clear documentary evidence that employees have been educated on what constitutes unacceptable conduct relating to harassment, discrimination, and bullying should assist in this regard.

There is no statutory grievance procedure under the Labour Law, or any statutory obligation to consider an employee's grievance, unless the grievance is in relation to a penalty imposed by the employer. However, it is often in an employer's interests to investigate an employee's complaint, particularly where it is of a serious nature. Where an employer has an internal grievance procedure, this should be followed.

There is also a general duty under the Penal Code to report a crime that has been committed. If the outcome of an employer's internal investigation confirms that an employee has harassed or bullied a co-worker in a way that constitutes a criminal offence under the Penal Code, the employer may be duty bound to report this matter to the police.

Where allegations of harassment, discrimination, or bullying are upheld, an employer will likely wish to take disciplinary action against the relevant employee. The employer should follow its own internal procedures in this regard, bearing in mind the requirements for termination of services of an employee under either Article 42 or Article 44 of the Labour Law (see [Enforceability](#)).

It is unlikely that a distinction will be drawn between bullying or harassment in person or via social media channels, as both types of conduct may breach UAE laws. As a result, the employer should take the same actions as those described above.

Business contacts

As long as the employee has consented in writing to be bound, an employer's policies can prohibit its employees from adding business contacts made during the course of their employment to personal social networking accounts. For the employer to take

disciplinary action in circumstances where an employee breaches this requirement, it will need to show that damage has been occasioned to the business as a result of this breach, and this will be difficult to prove (see *Enforceability*).

It is standard practice to include confidentiality clauses in employment contracts. Confidential information may include all information relating to the business of the employer and/or information relating to the business of the clients or customers of the employer. Details of business contacts may be considered part of the employer's confidential information.

In its policies, an employer can also 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.

Recruitment

Employers are entitled to use internet searches to perform due diligence on candidates in the recruitment process. Recruiting employers can rely on information obtained from a prospective employee's social media activity.

It should be noted that in the UAE, an employer would rarely, if ever, be in a position where it would have to justify its decision to reject a prospective employee, so the employer might not need to use a candidate's social media activity to inform its decision in any event. This is because persons who are not hired will face issues pursuing a claim; once a person is hired and becomes an employee, they can enforce their rights by way of a grievance filed with the local authorities. However, this avenue is available only to an employee who holds a labour permit under the provisions of the Labour Law.

If an employer refused to hire a candidate and this refusal was based on a prohibited reason (such as the applicant's religion), the candidate would have to make a complaint to the authorities under the Anti-Discrimination Law. This might lead to the imposition of sanctions on the would-be employer, but it is not likely to lead to an order to hire the candidate.

Discrimination on the following grounds is unlawful in the UAE:

- Religion.
- Creed.
- Doctrine.
- Sect.
- Caste.
- Race.
- Colour.
- Ethnic origin.

(Article 6, Anti-Discrimination Law.)

An employer may be held liable for the discriminatory actions of its employees where it had knowledge of the employee's discriminatory conduct (Article 17, Anti-Discrimination Law).

In addition, under Article 4 of the Labour Law, it is prohibited to "discriminate on the basis of race, colour, sex, religion, national origin, social origin or because of disability, which would impair equal opportunities or prejudice equality in obtaining or continuing a job and enjoying the rights".

As a result, if a prospective employee were able to prove that the would-be employer decided not to hire the candidate for an impermissible and discriminatory reason that it learned of from the candidate's social media activity, the prospective employee could possibly bring a complaint for breach of the Anti-Discrimination Law. However, although these protections against discrimination exist, the fact remains that an employer's decision not to hire a candidate is never reviewed in practice.

References

In its policies, an employer can prevent its staff from providing references for other staff on social media and professional networking sites.

Monitoring

Legal Requirements

As such, employee consent or notice is not then required, but it is best practice for the monitoring to be stated in the IT and social media policies. As noted previously, to be enforceable these policies will need to form part of the employee's employment contract (or be incorporated into it by reference) (see [Enforceability](#)).

The employer's IT policy can state that the employer can retrieve the contents of email messages and check internet usage by employees in the interests of the business in the following circumstances:

- To monitor whether use of the email system or the internet is legitimate and in accordance with the employer's IT and social media policy.
- To find lost messages or to retrieve messages lost due to computer failure.
- To assist in the investigation of alleged wrongdoing.
- To comply with any legal obligation.?

Employers can also monitor emails passing through their systems for viruses.

Internet postings and social media use by employees can be monitored by employers where the employee has chosen to make these publicly available. However, different considerations apply if the employer wishes to monitor purely private communications of an employee. In this case, the fact that such monitoring is in place should be clearly stated in the policies, as the employer could be found to be in breach of privacy laws or the Penal Code if the employee does not consent to the monitoring.

It is entirely untested whether it is permissible to monitor IT communications beyond the scope of what a user actually consents to or is even aware of; "eavesdropping" on the content of communications will be prohibited, but general monitoring of IT traffic to detect patterns (through cookies, for example) will probably be acceptable on the basis that the user consents to what the cookie does.

There are criminal offences in relation to the interception or disclosure of:

- Correspondence or telephone conversations (Articles 431, 432, and 433, Penal Code).

- Probably, IT communications (Article 12, Cyber Crimes Law).

See also the discussion of privacy rights in the Cyber Crimes Law under *Employee's Rights* which interact with the issue of monitoring.

An employee's agreement to monitoring waives only the employee's privacy rights, and has no effect on the privacy rights of the other parties to the employee's communications. Therefore, a blanket monitoring of private communications should be avoided, because it would infringe on the privacy not only of the employee who is being monitored but also the third parties with whom the employee communicates. The concern here is that a criminal invasion of privacy could be committed. Data privacy is also an issue, but a less acute one.

Automated Software

In the UAE, the employees' use of the employer's IT and communications systems can be continually monitored by automated software.

Investigations

- Subject to the above requirements, the employer may use information discovered during monitoring in retrieved emails or internet usage checks in an investigation of employee wrongdoing. Any information gathered during monitoring and can be passed to the following parties can be passed to:
 - Internal managers and staff.
 - External parties to conduct an independent enquiry or investigation.
 - The police for their criminal investigation into an employee.
- However, it is advisable that the employer's right to share relevant information for these purposes is expressly stated in the IT and social media policies.

CCTV

Installing CCTV in public areas such as on the exterior of the workplace premises is permissible, subject to compliance with any laws applicable in the relevant Emirate. For example, in Dubai, employers must apply for permission from the police before installing the device in their premises.

Recording employees inside the workplace is also allowed, but it is advisable that the employees are notified and their consent is obtained beforehand.

ChatGPT

There is currently no legislation or statutory guidance on the use of Generative AI or ChatGPT or the restrictions/ that can be put in place to circumscribe its use. However, ChatGPT has already been adopted by government entities such as the Telecommunications and Digital Government Regulatory Authority. Similarly, the Dubai Electricity and Water Authority announced that it is working to utilise ChatGPT to enhance its services.

However, artificial intelligence tools such as ChatGPT are known to be used to spread misinformation or fake news, as well as to cause privacy and data protection issues. Therefore, it is permissible for an employer to restrict the use of Generative AI and ChatGPT in its IT and social media policies. The scope of the restrictions will largely depend on the type of organisation and the type of services it offers to its clients.

ChatGPT restrictions can be included in the general IT and social media policies; however, in certain specialised sectors (such as the legal sector) which require the use of ChatGPT to be controlled, or have witnessed a rampant misuse of ChatGPT, employers may consider introducing content relating to ChatGPT as a separate policy.

END OF DOCUMENT

Related Content

Tasks

[Employing people in banks](#)

Practice note: overview

[Overview of Labour Laws \(United Arab Emirates\)](#)