LEGALSKILLS

an online learning platform

SOCIAL MEDIA IN THE WORKPLACE

BY AALIA MAHOMED

COURSE OVERVIEW

In this course, you will:-

1. Understand the importance of using social media to conduct business
2. Learn how to adopt good social media practices
3. Understand the components of a social media policy
4. Understand the legal implications of the misuse of social media
5. Have practical guidelines to monitor social media practices

SECTION ONE:

BENEFITS OF SOCIAL MEDIA TO CONDUCT BUSINESS

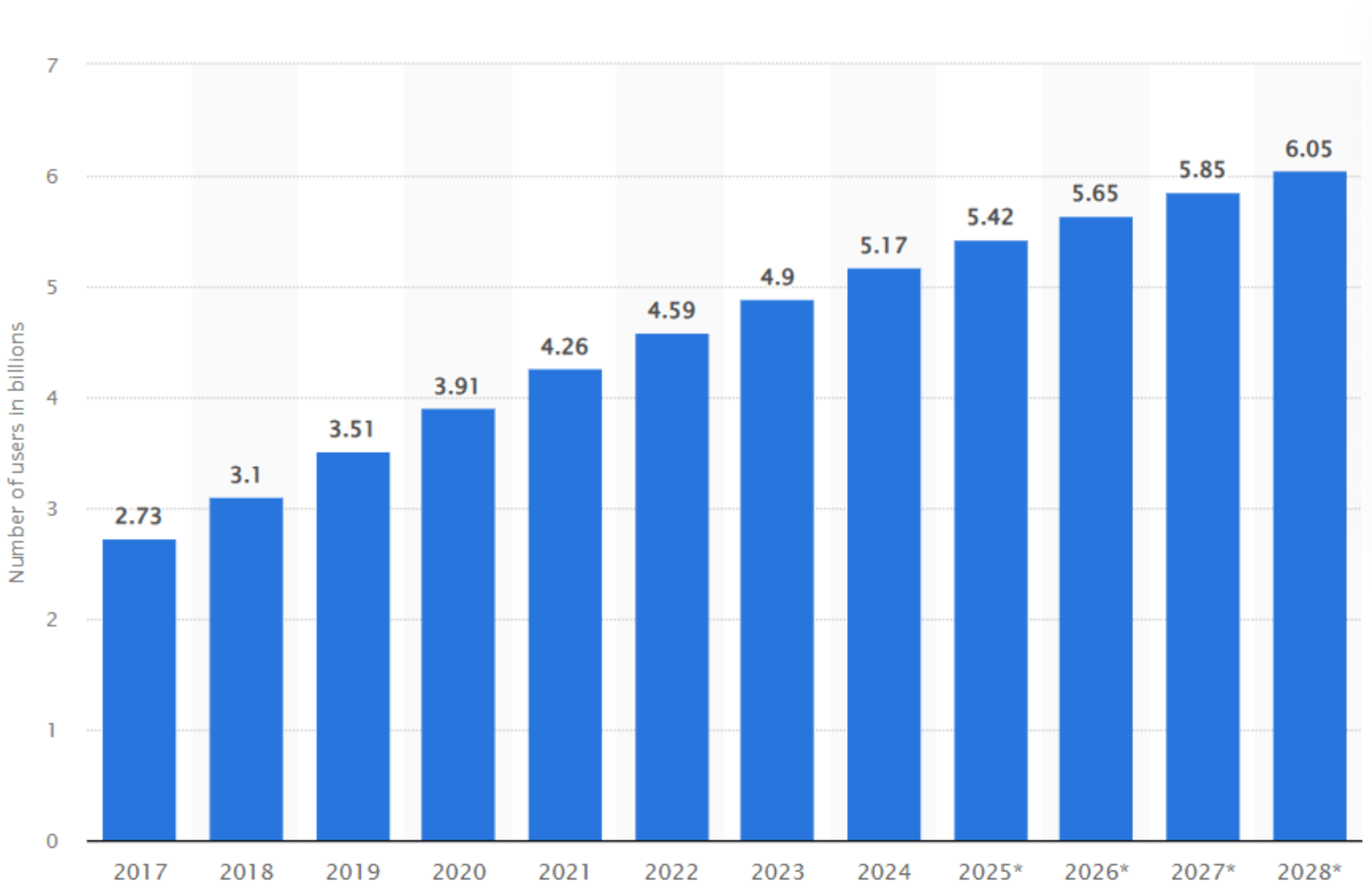
BENEFITS OF SOCIAL MEDIA

- Social media is a powerful tool that has revolutionised how companies communicate and conduct their businesses
- Social media platforms include (but are not limited to): X (formerly Twitter), Instagram, LinkedIn, YouTube and Facebook which companies use to engage with their **target audience, namely consumers, employees, future recruits and other stakeholders**
- Research by Global WebIndex indicated that "*63.8% of the world's population uses social media. The average daily usage is 2 hours and 19 minutes (October 2024).*" Companies are aware of the exponential growth of users on social media platforms and strategically leverage social media to their advantage





USE OF SOCIAL MEDIA



- This graph represents the *number of social media users worldwide from 2017 to 2028 (in billions)* as predicted by Statista in 2024
- Social media has become an essential feature of business today and cannot be avoided
- By 2028, Statista predicts there will be approximately 6.08 billion users on social media. This reinforces the importance of companies adopting social media in their business

BENEFITS OF SOCIAL MEDIA

- INCREASE IN REVENUE
- IMPROVE CUSTOMER ENGAGEMENT AND CUSTOMER SERVICE
- BUILD A STRONG CREDIBILITY AND REPUTATION FOR THE BUSINESS
- EASY COMMUNICATION WITH ITS TARGET AUDIENCE
- COMPETITIVE ADVANTAGE
- BRAND AWARENESS
- BUILD TRUST AND LOYALTY WITH CUSTOMERS
- COST-EFFECTIVE MARKETING TOOL
- STRENGTHENS EMPLOYEE ENGAGEMENT
- COMPREHENSIVE INSIGHTS AND ANALYTICS

The benefits of social media are extensive and transformative for companies

Companies that can leverage social media to their advantage create value and they reap these benefits by implementing good social media practices

SECTION TWO:

HOW TO ADOPT GOOD SOCIAL MEDIA PRACTICES

STEP 1: BE STRATEGIC

A company must adopt and maintain good social media practices to use social media effectively. The following steps will assist in adopting good social media practices:-

- Identify the **goals** of the company and how social media can strategically achieve these goals
- Identify the company's **target audience** and how they can be reached
- Identify the **brand** of the company that you wish to establish online
- Identify which **social media platforms** are appropriate for the company
- Establish the social media goals of the company

STEP 2: CREATE A SOCIAL MEDIA TEAM

- Create a *Social Media* team within the company to manage the company's social media platforms
- Appoint an individual employee as the *Social Media Manager* to manage the Social Media Team and assist employees using social media platforms
- The Social Media Team will be solely responsible for and authorised to publish any content on behalf of the company online. This team will exclusively manage all online engagements on the company's social media platforms
- The Social Media Team will:-
    - engage with employees regarding social media training and any queries
    - ensure the company's brand is accurately represented online
    - identify trends and opportunities online to benefit the company
    - monitor customer engagements
    - address customer concerns and dissatisfaction posted online
    - report any reputational risks

STEP 3: CREATE A TONE FOR THE COMPANY ONLINE

- The company’s tone online will establish the company’s personality and brand
- Determine the type of content to be posted on the company's social media platforms and consider its impact on the company
- It is important to maintain a uniform tone with the company’s interactions online to connect with its target audience
- It is recommended that all content published on social media platforms have been thoroughly evaluated and re-evaluated by the Social Media Team before publishing online

STEP 4: CREATE A SOCIAL MEDIA POLICY

- A social media policy ("**SC Policy**") is a document that regulates the use of social media by employees for professional and personal purposes
- Employees can help build the company's brand on social media. However, the company needs to ensure that employees are properly trained to represent the company online positively
- An SC Policy includes a set of guidelines for employees to follow when using social media. This document can guide employees on how they represent themselves online, both personally and professionally in association with the company
- **Note**: A SC Policy will provide disciplinary measures for employee non-compliance, such as dismissal. Having a comprehensive SC Policy will support a fair dismissal of an employee in the event he/she brings the company's reputation into disrepute by using social media

STEP 5: MAINTAIN GOOD SECURITY MEASURES

- Ensure that access and control to the company's social media platforms are managed exclusively by the Social Media Team
- Restrict access to company passwords on social media platforms to specific individuals within the Social Media Team i.e. the Social Media Manager
- Encourage good security measures to be adopted by employees such as two-step authentication and strong passwords for their devices and social media platforms

STEP 6: MAINTAIN GOOD SOCIAL MEDIA PRACTICES

- Employees should be adequately trained on the use of social media platforms and ensure that training materials and the SC Policy are available and accessible at all times
- While having an SC Policy is important to regulate social media usage, employees must be aware of this policy and fully understand what actions amount to inappropriate behaviour on social media and the consequences thereof
- Training of employees should take place regularly and the company should set performance indicators to evaluate employee training
- Encourage employees who are engaging correctly on social media

SECTION THREE:

CREATING A SOCIAL MEDIA POLICY

WHAT IS A SOCIAL MEDIA POLICY?

What is a Social Media Policy?

- This policy includes guidelines to be followed by employees when using social media for personal or professional purposes
- What is the purpose of a social media policy ("**SC Policy**")? This policy will:-
  - educate and inform employees that their interactions on social media platforms could have a negative impact on the company
  - advise employees on conduct that is not permissible on social media platforms
  - inform employees of the consequences and disciplinary measures for a breach of the SC Policy
  - assist in mitigating risks associated with social media

ESSENTIAL COMPONENTS OF AN SC POLICY

1. DEFINE SOCIAL MEDIA

- Include a definition of social media
- Refer to the social media platforms used by the company and its employees to promote its services to its target audience
- Inform employees of the consequences of using social media platforms, specifically that:-
  - that content posted on social media is permanent
  - actions taken by the employee could be a reflection of the company
  - there is a wide scope for reputational harm for the company
  - there can be legal implications for actions taken on social media platforms

ESSENTIAL COMPONENTS OF A SC POLICY

2. DEFINE THE PURPOSE OF THE POLICY

The purpose of the SC Policy should include:-

1. **Rules and guidelines**
2. **Roles and responsibilities** of employees
3. **Identify confidential information**
4. **Consequences** for any non-compliance with the SC Policy

ESSENTIAL COMPONENTS OF AN SC POLICY

3. RULES AND GUIDELINES FOR EMPLOYEES

The guidelines should be comprehensive and provide for:-

- the creation of social media accounts by employees
- the management of personal social media accounts by employees
- posting content regarding the company, its employees, customers and other stakeholders
- any queries or concerns by employees regarding social media
- social media training

ESSENTIAL COMPONENTS OF AN SC POLICY

3. RULES AND GUIDELINES FOR EMPLOYEES

Please see the below examples of guidelines to be included in the SC Policy:-

- When creating a social media account employees may not use their company email address to set up their account. An employee's personal email account must be used to register for any social media platforms or online tools for their personal use
- Employees in their personal or professional capacity, may never share or refer to confidential or proprietary information of the company on their social media platforms
- Employees who post content on social media platforms should disclose that their content reflects their personal views and does not reflect the company's views. It should be clear that the content posted by the employee is not in association with the company in any form
- Employees may not share any content (such as photos) of the company’s employees on their social media platforms unless they have obtained their prior written approval

ESSENTIAL COMPONENTS OF AN SC POLICY

4. ROLES AND RESPONSIBILITIES OF EMPLOYEES

- Identify the members of the Social Media Team and include their contact details
- Inform employees of the role of the Social Media Team and should any employee have (i) concerns or queries regarding social media; or (ii) require social media training, such requests should be referred to the Social Media Team

ESSENTIAL COMPONENTS OF AN SC POLICY

5. CONFIDENTIAL INFORMATION

- Emphasise the importance of keeping the company's proprietary information confidential
- Provide specific examples of what would constitute confidential information, see the examples below:-
    - Information related to promotions or salaries
    - Information regarding the company’s clients
    - Strategic planning of the company
    - Information regarding the appointment of new staff (unless confirmed and made public by the company on its social media platforms)
- The rule of thumb is that employees should only share public information about the company or have obtained the necessary approvals (e.g. from the Social Media Team or the relevant supervisor) before publishing any content online

ESSENTIAL COMPONENTS OF A SC POLICY

6. NON-COMPLIANCE WITH THE SC POLICY

- It is important to inform employees that there can be legal implications for their engagements on social media platforms
- More importantly, failure of an employee to adhere to the SC Policy will result in disciplinary action against the relevant employee
- Disciplinary action could include the issue of a formal warning or dismissal, depending on the severity of the transgression by the relevant employee

SECTION FOUR:

LEGAL IMPLICATIONS OF SOCIAL MEDIA

LEGAL IMPLICATIONS OF SOCIAL MEDIA

- Social media misconduct by an employee may amount to defamation, sexual harassment or the disclosure of confidential and private information which may cause harm to the employer in terms of reputation and/or economic loss

- Several applicable laws come into play when using social media, including but not limited to:-

  - The Prevention and Combating of Hate Crimes and Hate Speech Act 16 of 2023 – this act criminalises hate crime and hate speech

  - The Cybercrimes Act 19 of 2020 – describes "*malicious communications*" and criminalises certain actions forming part of malicious communications such as data messages sent by any person (via electronic communication) to another person (or group of persons) which (i) incites damage to property or violence; and (ii) which threatens persons with damage to property or violence. Additionally, malicious communications include the disclosure by any person of data messages of an intimate image

  - Criminal offence, *Crimen injuria* - *Crimen injuria* is the act of unlawfully and intentionally impairing the dignity or privacy of another. Should an employee post abusive or degrading communications related to defamation, such actions may lead to a criminal offence of *Crimen injuria* if the requirements of the offence are met

IMPORTANT CONSIDERATIONS

In this section we will answer the following questions:

1. Can an employee raise the constitutional right to privacy as a defence for social media misconduct?
2. How can an employee be held liable for defamation as a result of social media misconduct?
3. When can an employer be held vicariously liable for its employees' misuse of social media?
4. How can the misuse of social media lead to privacy violations in the context of the Protection of Personal Information Act otherwise known as "**POPIA**"?

THE RIGHT TO PRIVACY

- The right to privacy (Section 14 of the Constitution) provides that everyone has the right to privacy which includes the right not to have the privacy of their communications infringed
- The right to privacy is not absolute, should an employee raise the right to privacy when faced with sanctions as a result of their social media misconduct, their rights may be limited
- In the case of *Gaertner & others v Minister of Finance & others* 2014 (1) BCLR 38 (CC), the court held that:-

  "Privacy, like other rights, is not absolute. As a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks"

THE RIGHT TO PRIVACY

- Refer to the case of *Sedick & Another v Krisray (Pty) Ltd* [2011] 8 BALR 879 (CCMA), a brief overview of this case is as follows:-
  - The two applicants, Sedick and De Reuck (collectively the "**Applicants**") were dismissed from their employment for bringing their employer's name into disrepute;
  - The Applicants were dismissed for posting derogatory statements on Facebook about the owner and members of his family employed by the respondent;
  - The Applicants challenged the decision of their dismissal by their employer. The Applicants held that the comments in question did not specifically refer to the company, nor was any member specifically named. In addition, the Applicants raised that **their privacy had been breached** by the employee who accessed their Facebook pages; and
  - The commissioner held that:-
    - Facebook is open to the public and members can set their desired privacy settings. In other words, the Applicants chose not to restrict access to their Facebook pages;
    - the respondent was therefore entitled to intercept the comments made by the Applicants;
    - given that there was open access to the comments, it had the potential to damage the reputation of the employer including its customers, suppliers and competitors; and
    - the dismissal of the Applicants was procedurally and substantively fair in these circumstances

THE RIGHT TO PRIVACY

- An important takeaway from this case:-

  An employer's access to the social media account of an employee will not infringe on the employee's right to privacy if the employee does not restrict access to the comments made on their social media

- **Note**: Employers may not unlawfully intercept private social media accounts or personal emails. The admissibility of unlawfully obtained information will be determined by the court and in some instances it may amount to a violation of privacy

THE RIGHT TO PRIVACY

Refer to the case of *Harvey v Niland and Others* (ECG) 5021/2015 (unreported), a brief overview of the case is as follows:

- Harvey ("**Applicant**") and Niland are the only members of Huntershill Safaris CC ("**Huntershill**");
- Harvey had instituted an urgent application to interdict Niland from causing financial and reputational harm to Huntershill;
- Niland resigned from Huntershill as an employee and continued to hold his member's interest in the close corporation and therefore continued to owe a fiduciary duty to Huntershill;
- Niland was subsequently employed at a competitor of Huntershill and posted on his Facebook page that he was *'going onto bigger thinking*' and would continue at "*a company not far from here*";
- Harvey had the password to Niland's Facebook account and accessed his account without his knowledge. Harvey printed the communications of Niland and submitted these posts in support of his application to obtain an interdict at the High Court;
- The communications indicated Niland's attempts to solicit clients from Huntershill; and
- The court held:-
    - the court has to exercise discretion to exclude unlawfully obtained evidence;
    - it was clear from the communications of Niland that he had breached his fiduciary duties owed to Huntershill by undermining its business; and
    - there was no other means by Huntershill to provide evidence of Niland's wrongdoing without obtaining access to this communication to enforce its rights against Niland

THE RIGHT TO PRIVACY

- <u>An important takeaway from this case:-</u>
  - The right to privacy is not absolute. In some circumstances unlawfully obtained information may be admissible if the employer has no other means to protect the interests of the company
  - The right to privacy should not be relied on by employees seeking to avoid the repercussions of social media misconduct

DEFAMATION

DEFAMATION

- The right to freedom of expression is a constitutional right which affords one the right to express oneself freely. However, this right is not without limitations, employees may not use social media as a means of expressing themselves in a manner that would harm their employer

- The law of delict provides recourse for a person to claim compensation from another for harm that has been suffered as a result of another. Should an employee post derogatory statements or content on social media platforms (including messages), such communications may give rise to a claim for defamation under the law of delict

- How to prove that a derogatory or untrue statement regarding the employer or connected to the employer is defamatory: A statement in this context is defamatory if it has the effect of **injuring the employer's reputation**. For the employer to hold the employee liable, it would have to prove the employee's conduct amounted to defamation, namely that the conduct was:-

    - **Wrongful** – there must be harm or injury
    - **Intentional** – the employee must have intended to defame the employer;
    - **Published** – the statement should have been published (verbal or written);
    - **A defamatory statement** – must exist which violates the reputation of the employer; and
    - **Related** – to the employer

DEFAMATION

Dismissal of an employee for defamation

- Defamatory statements by an employee that have the result of damaging the employer's business is an act of misconduct. The Labour Relations Act 66 of 1995 (as amended) provides that misconduct is a ground for dismissal

- In the case of *Makhoba v Commission for Conciliation, Mediation and Arbitration and Others* (1280/17) [2021] ZALC 11 an employee was dismissed from the company for posting a racist statement on Facebook. A brief overview of this case:-

    - Mr Makhoba was an employee of Clover;
    - After posting a racist statement online, Mr Makhoba was dismissed from his employment after undergoing arbitration proceedings in 2017;
    - In 2021 Mr Makhoba submitted an application to the Labour Court to be reinstated in his position at Clover;
    - Mr Makhoba relied on the defence that he had posted the statements while he was "off-duty";
    - The court confirmed that **an employer can exercise discipline over an employee for off-duty misconduct if there is a connection between his conduct and the employment relationship;**
    - The court held that Mr Makhoba acted contrary to the company's interests by exposing the company to the risk of reputational damage; and
    - The application was dismissed on the basis that the sanction of dismissal was appropriate in these circumstances

DEFAMATION

- An important case with noting is *Edcon Limited v Cantamessa and Others* (JR30/17) [2019] ZALCJHB 273; (2020) 41 ILJ 195 (LC); [2020] 2 BLLR 186 (LC). This case has a similar set of facts where an employee, Ms Cantamessa was dismissed from Edcon for posting racist statements on her Facebook social media account

- The court held that:-
  - the fact that the misconduct by the employee took place away from the workplace does not preclude the employer from disciplining the employee, provided that Edcon can **establish the necessary connection between the misconduct of Ms Cantamessa and its business**;
  - although the comments by Ms Cantamessa did not relate to Edcon, the only source of connection between her and Edcon was that her Facebook profile indicated that she worked for Edcon;
  - Edcon operates in a competitive industry and its success largely depends on how it markets itself. **Maintaining a good name and reputation is an essential asset or quality of Edcon**;
  - **Ms Cantamessa had a duty to avoid being a controversial employee in the public eyes where she could be associated with Edcon**; and
  - Ms Cantamessa's dismissal in these circumstances was an appropriate sanction by Edcon

DEFAMATION

An important takeaway from the above cases:

- Employees should be aware that their personal or professional engagements online, whether during business hours or not, could be linked to the company
- Should an employee post inappropriate or derogatory content online, this action could give rise to serious misconduct that would result in dismissal

VICARIOUS LIABILITY - DEFAMATION

VICARIOUS LIABILITY

- The doctrine of vicarious liability exists in our Common Law. It recognises that another party may be held liable for the delict of the perpetrating party which has caused the loss of a third party. This means that an employer can be held liable for the misuse of social media by their employees if the requirements for vicarious liability have been met

- The requirements for an employer to be vicariously liable for the delict of their employee are as follows:-

    1. There must be an employer-employee relationship at the time of the commission of the delict;
    2. The employee must commit a delict causing loss to a third party; and
    3. The employee must have been acting within the scope of his duties at the time that the delict was committed

- An employer's vicarious liability will be determined by the court having regard to the facts of the case

VICARIOUS LIABILITY - DEFAMATION

- In the case of *Stallion Security (Pty) Limited v Van Staden* (2019) ZASCA 127, the court confirms the test for vicarious liability as follows:-

> *"[T]he test is one which contains both a factual assessment (the question of the subjective intention of the perpetrators of the delict) as well as a consideration which raises a question of mixed fact and law,* ***the objective question of whether the delict committed is "sufficiently connected to the business of the employer" to render the employer liable****."*

In addition, the court held:-

  - that a sufficiently close link must exist between the wrongful act of the employee on the one hand and the business or enterprise of the employer; and
  - whether the employer had created the risk of the harm that materialised, must be determined objectively

- With regards to the misuse of social media by employees, an employer cannot avoid liability by claiming that they did not allow or authorise inappropriate publications by employees using social media. An employer must ensure that employees are adequately trained on social media activities that are inappropriate and prohibited by the company. The company must have taken steps to avoid the risk of social media misuse by its employees in the workplace

POPIA

PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013 - POPIA

- Everyone is afforded the right to privacy (in terms of Section 14 of the Constitution), this right includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. POPIA aims to protect an individual's right to privacy in this regard

- Important terminology to note (as defined in the POPIA):-
  - ‘‘**Data Subject**’’ means the person to whom personal information relates;
  - ‘‘**Person**’’ means a natural person or a juristic person;
  - ‘‘**Processing**’’ means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including —

    (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

    (b) dissemination by means of transmission, distribution or making available in any other form; or

    (c) merging, linking, as well as restriction, degradation, erasure or destruction of information;
  - ‘‘**Responsible Party**’’ means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

POPIA

- Important terminology (as defined in the POPIA) continued:-
  - "**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

    (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

    (b) information relating to the education or the medical, financial, criminal or employment history of the person;

    (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

    (d) the biometric information of the person;

    (e) the personal opinions, views or preferences of the person;

    (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

    (g) the views or opinions of another individual about the person; and

    (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

POPIA

- A company conducting its business will have access to the personal information of its employees, clients and stakeholders. In this instance, the company is regarded as a *Responsible Party* and will be required to comply with the lawful conditions for processing personal information as contemplated in POPIA

- The lawful conditions for processing personal information include:-

ACCOUNTABILITY	INFORMATION QUALITY
PROCESSING LIMITATION	OPENNESS
PURPOSE SPECIFICATION	SECURITY SAFEGUARDS
FURTHER PROCESSING LIMITATION	DATA SUBJECT PARTICIPATION

POPIA

See below for a further explanation of the lawful conditions for processing personal information:-

1. **Accountability** – the company/organisation is required to comply with the lawful conditions for Processing Personal Information as contemplated in POPIA
2. **Processing Limitation** – Personal Information must be processed in a lawful manner that does not infringe the privacy rights of a Data Subject
3. **Purpose Specification** – Personal Information may only be Processed for a specific, explicitly defined and lawful purpose
4. **Further Processing Limitation** – further Processing of Personal Information must be compatible with the purpose for which it was collected
5. **Information Quality** – the company/organisation must ensure that the Personal Information is complete, accurate, not misleading and updated where necessary
6. **Openness** – the company/organisation must document its Processing activities and provide adequate notice to the Data Subject of its Processing activities
7. **Security Safeguards** – the company/organisation must secure the integrity and confidentiality of the Personal Information in its possession or control. Preventative measures include:- protection against loss of, damage to or unauthorised destruction of Personal Information and unlawful access
8. **Data Subject Participation** – the company/organisation must ensure that the Data Subject's right to access, correct or delete Personal Information is upheld

POPIA

- A company therefore has very stringent and specific requirements to follow when the Personal Information of its clients, stakeholders and employees is in its possession or under its control
- It is of utmost importance that employees are informed of the company's compliance with POPIA during their training sessions. This will avoid the risk of Personal Information being released on social media platforms
- **Note**: Should the company fail to comply with the provisions of POPIA, the company may be liable for administration and/or financial fines in terms of POPIA. Furthermore, its non-compliance will have a detrimental effect on the company's reputation, resulting in the loss of clients, investors or employees

POPIA

- The case of *Munetsi v Madhuyu and Another* (16255/2024) [2024] ZAWCHC 209 deals with the publication of Personal Information on social media

- A brief overview of this case:-

  - Mr Munetsi (the "**Applicant**") approached the Cape Town High Court for an urgent interdict against Mr Madhuyu and Ms Tonsani (the "**Respondents**");
  - The Applicant alleged that the Respondents had breached the provisions of POPIA by publishing his cell phone number on their social media platforms, Facebook and TikTok;
  - The Respondents had a large following on their social media platforms; and
  - The Respondents published the cell phone number of the Applicant online and requested their viewers to call the Applicant

- According to the provisions of POPIA "*personal information*" includes the "*telephone number*" of an "*identifiable, natural, living person*". The court held that *personal information* may only be "*processed*" (as defined in POPIA) in specific circumstances set out in POPIA. *Specific circumstances,* in this regard, refer to the condition of Purpose Specification (Section 11 of POPIA) which provides that *personal information* may only be processed for a specific, explicitly defined and lawful purpose

- The court held that the Respondents had breached POPIA by publishing the Applicant's cell number on social media without a lawful basis

- <u>An important takeaway from this case:</u> a company as a Responsible Party requires a lawful purpose for Processing Personal Information

SECTION FIVE:

IMPLEMENTATION AND MONITORING

IMPLEMENTATION & MONITORING

- At this stage of the course, you have understood the importance of social media and the need to regulate its use by employees within the workplace. Additionally, you would have understood the important role of social media training and adopting a Social Media Policy

- In this section, you will identify how to maintain good social media practices through implementation and continuous monitoring:-

- **<u>Implementation of social media policy</u>**
    - Employees should be aware of the contents of the social media policy
    - Incorporate training on social media policies during the onboarding of new employees
    - Provide for regular review (i.e. annually) of the social media policy and update where necessary
    - Keep abreast of developments in the law which would require updates to the social media policy
    - Provide adequate notice to employees on updates to the social media policy
    - Ensure that the latest version of the social media policy is accessible to employees at all times

IMPLEMENTATION & MONITORING

Monitor social media channels

- Regularly monitor social media channels for negative or false statements regarding the company and its employees
- Monitor employees' social media interactions if publicly available – specifically on professional social media platforms such as LinkedIn
- **Note**: Employers may not require that employees provide them access to their private social media accounts

Reduce the use of social media during work hours

- Limit the use of social media during work hours by determining which websites are acceptable for conducting business and limiting access to certain social platforms
- It is permissible to monitor the internet sites visited by the employee provided the employer has obtained consent to monitor their electronic communications for business purposes. **Note**: it is common practice to obtain general consent from an employment contract

LEGALSKILLS+

an online learning platform

SOCIAL MEDIA IN THE WORKPLACE

BY AALIA MAHOMED