Evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff

submitted in fulfilment of the requirements of the degree of

Master of Management Sciences in Administration and Information Management

in the

Faculty of Accounting and Informatics

at the

Durban University of Technology

by

Nonhlanhla Beata Mkhize

Date Submitted: 5 December 2022

Supervisor: Dr CJ Nyide

(DBA: Finance) Date: 2/12/2022

Co-Supervisor: Dr PP Mthalane

(PhD: Public Management) Date: 2/12/2022

DECLARATION

I, Nonhlanhla Beata Mkhize, declare that this dissertation is a representation of my work in conception and execution. This work has not been submitted in any form for another degree at any university or institution of higher learning. All information cited from published or unpublished works has been acknowledged.

Signature

_____ _____ **2/12/2022**

Date

APPROVED FOR FINAL SUBMISSION

2/12/2022

Supervisor's name Dr NJ Nyide Date

(DBA: Finance)

2/12/2022

Co-supervisor's name Dr PP Mthalane Date

(PhD: Public Management)

ABSTRACT

Computer technology and the Internet have improved communication and productivity across organisations. Regardless of the many advantages that the Internet has brought to organisations, cyber-loafing is a serious challenge that many organisations are faced with. This habit has increased in such a way that it has negatively impacted the organisation's productivity because employees are skipping their duties as they engage in cyber-loafing. Furthermore, this act leaves organisations in a vulnerable position, exposing the company to serious risks of breaching security policies. With the advent of the Fourth Industrial Revolution, the Internet and computer technology will continue to play a pivotal role and companies will continue to face serious problems dealing with cyber-loafing during work hours.

Organisations are reported to have put in place systems to reduce cyber-loafing, such as software programmes designed to monitor, track and lock down the illegal use of the Internet. Unfortunately, these systems do not completely prevent employees from engaging in cyber-loafing; hence, the role of managers in mitigating this act cannot be ignored. The role played by managers in reducing and controlling cyber-loafing is not clear. Therefore, the purpose of this research was to evaluate tools used by managers to prevent and control cyber-loafing by administrative staff in the workplace and suggest effective tools that can be put in place to mitigate this phenomenon. This study employed a mixed method, which combines the elements of qualitative and quantitative research approaches. This method was considered necessary to gain an in-depth understanding of the phenomenon and to strengthen the validity of the findings. Using purposive sampling, the sample size for the quantitative study was 156 administrative staff and the sample size for the qualitative part of the study was 11 managers and supervisors.

The results of this study demonstrate that there are major and minor cyber-loafing activities among the investigated administrative staff. Sending and receiving

emails were ranked highest among cyber-loafing deeds. Other major cyber-loafing activities found were visiting holiday and travel websites, visiting social media sites, pursuing studies, accessing online news, accessing auction sites and checking weather forecasts. The least popular activities were accessing online magazines, gaming and sports and shopping. The results from the quantitative data also revealed that administrative staff at the research site acknowledge that there are some tools used at their workplace to control cyber-loafing activities. Findings from qualitative data corroborate the quantitative results. This triangulation process indicates that managers and supervisors have strategies in place to combat cyber-loafing among administrative staff. Some managers and supervisors keep an eye on their employees and walk around them while they work. Whilst managers and supervisors employ some tools to curb cyber-loafing activities within the organisation, it is the responsibility of the ICT department to monitor internet usage and block websites.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisors, Dr. Nyide and Dr. Mthalane, for their patience and guidance throughout this journey.

Furthermore, I would like to thank everyone who took the time to participate in this study. Their contribution is greatly appreciated.

To my family, thank you for allowing me to further my studies and pursue my dreams. Your guidance and unwavering support are unmatched. I appreciate you.

Finally, I'd like to thank the Lord Almighty for giving me strength and sustaining me when I was ready to give up.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION AND OVERVIEW OF THE STUDY

1.1 INTRODUCTION

Organisations are faced with the challenge of employees who use the internet for their personal use during work hours. This negatively affects work productivity, network security and bandwidth losses. There are estimates of billions of rands lost due to production loss, internet expenses, and security problems, making cyber-loafing a significant challenge for many organisations. Irrespective of several mechanisms employed by managers to mitigate cyber-loafing among employees, this behaviour remains a challenge in many organisations. This introductory and overview chapter provides contextual information outlining the background of this research. It unpacks the problem statement, its aim and objectives, as well as the research questions.

1.2 BACKGROUND TO THE STUDY

Computer technology and the Internet have eased and improved communication across organisations (Jandaghi, Alvani, Zarei and Fakheri 2015: 5). These technological resources have not only improved the method of communication, but they have also boosted productivity and enhanced operational processes. While this great innovation of the Internet, computer and network is increasing, employees, on the other hand, have developed new strategies for escaping their work duties and using company computers and the Internet to perform non-work-related tasks during company hours (Elciyar and Simsek 2021: 56). This habit has increased to levels that have negatively impacted the organisations' productivity as more and more employees are skipping their assignments and engaging in cyber-loafing (Jandaghi 2015: 69). As a result, organisations are faced with a myriad of challenges, which include identity theft, time squandering

and a lack of creativity as a result of employees' fragmented focus during cyber-loafing (Kasap 2019: 36).

Although companies have discovered many tools to control cyber-loafing behaviour, the number of employees who engage in cyber-loafing continues to grow. According to research, managers lack the necessary skills and tactics for minimising workplace cyber-loafing (Abbasi 2018: 24; Kaptangil 2021: 56; Toker and Baturay 2021: 45). Some of these incidents are not properly addressed because of the cost of dealing with or resolving this behaviour by workers. To deal with the scourge of cyber-loafing, most organisations are using several tools and strategies as means of monitoring internet and computer usage. However, there is still a need to evaluate the effectiveness of the existing cyber-loafing tools to curb this plague (Hassan, Reza and Farkhad 2015: 19; Song, Ugrin, Li, Wu, Guo and Zhang 2021: 20). Therefore, the purpose of this research is to examine the tools used by managers to control cyber-loafing activities by administrative staff.

1.3 PROBLEM STATEMENT

Technology has become an indispensable part of our everyday existence. However, one cannot ignore the negative effects and consequences it has (Kanholkar and Dharkar 2022: 45). Regardless of the numerous advantages that the internet has brought to organisations, cyber-loafing is a serious challenge that many organisations are faced with. According to Al Abbasi (2018: 4), it is estimated that organisations have lost billions of rands due to production loss, internet costs and internet security issues due to cyber-loafing among administrative staff. This leaves organisations in a vulnerable position, negatively affecting company policy and exposing the company to serious risks of security breaches. Cyber-loafing also affects the employees' abilities and the quality of production in the long run (Al Abbasi, 2018: 4). It also encourages internet gambling, which wastes useful working hours (Pandey and Pandey 2021: 45). The internet and computers will continue to play a pivotal role the Fourth Industrial

Revolution. However, companies will continue facing serious problems in dealing with cyber-loafing among employees during work hours (Kanholkar and Dharkar 2022: 45).

Organisations are reported to have put systems in place to reduce cyber-loafing, such as software programmes designed to monitor, track, and lock illegal use of company internet facilities (Aku, 2017: 7). Unfortunately, these systems do not completely prevent employees from engaging in cyber-loafing; hence, the role of managers in mitigating this act cannot be ignored (Aku, 2017: 7). Previous research has concentrated on identifying various kinds of cyber-loafing behaviours among employees, classifying cyber-loafing into two categories: minor cyber-loafing and serious cyber-loafing (Tandon, Kaur, Ruparel, Islam and Dhir 2021: 97; Dooly 2021: 56; Aku 2017: 45; Khansa 2017: 54). However, there is no proof of studies that concentrated on an assessment of tools used by managers to regulate cyber-loafing by administration staff. Furthermore, Holgin (2016: 18); Tandon *et al.* (2021: 97) maintain that the effectiveness of tools used by managers in reducing and controlling cyber-loafing has not been evaluated nor has the need to discover new ones been fully investigated. Therefore, this study will evaluate tools used by managers to prevent and control cyber-loafing among administrative staff using eThekwini Municipality Sizakala Customer Care as a case study.

1.4 AIM OF THE STUDY

This study aimed to evaluate existing tools used by managers to prevent and control cyber-loafing among administrative staff in the workplace. The intention was to identify and suggest effective tools that can be put in place to mitigate this phenomenon. This was achieved by using eThekwini Municipality Sizakala Customer Care as a case study.

1.4.1 Research Objectives

The objectives of this research are to:

- identify cyber-loafing activities that are common among administrative staff at eThekwini Municipality Sizakala Customer Care;
- determine the tools used by management to control cyber-loafing activities by administrative staff at eThekwini Municipality Sizakala Customer Care, and
- examine factors affecting the implementation of tools that can be used by management to control cyber-loafing activities by administrative staff.

1.4.2 Research Questions

- What are the cyber-loafing activities that are common among administrative staff at eThekwini Municipality Sizakala Customer Care?
- What are the tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer Care?
- What factors affect the implementation of tools that can be used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer Care?

1.5 SIGNIFICANCE OF THE STUDY

It is without a doubt that cyber-loafing jeopardises organisations' efficiencies and security. As a result, managers strive to reduce the risks associated with employee cyber-loafing. These dangers include decreased output and the possibility of malware or other security issues. This research is important because it identifies and evaluates tools that managers can use to establish monitoring and deterrence mechanisms in their organisations. This study is expected to shed light on how managers can enhance the implementation of cyber-loafing deterrence strategies and tools. Furthermore, the findings of this study are expected to add value by contributing to the literature as far as this phenomenon is concerned.

1.6 RESEARCH METHODOLOGY AND DESIGN

Bhasin (2019: 14) explains that a research design is a step-by-step procedure that shows how a researcher conducts a scientific investigation. It includes methods and procedures for researching so that a research problem can be effectively managed (Kanholkar and Dharkar 2022: 45). The research design specifies the data collection strategy, the unit of analysis, the survey structure used for data collection and the type of outcomes the study seeks. A descriptive research design was used to achieve the aim and objectives of this study. Descriptive design is useful when describing the characteristics of an already known phenomenon (Pandey and Pandey 2021: 45). Moreover, a mixed method approach was employed in this study, which combines elements of qualitative and quantitative research. This method was considered appropriate to gain an in-depth understanding of the phenomenon and to strengthen the validity of the findings (Dudovskiy 2016: 10).

1.7 ORGANISATION OF THE STUDY

This study consists of five chapters. These chapters are organised as follows:

CHAPTER 1: INTRODUCTION AND BACKGROUND TO THE STUDY

This chapter introduced the study and unpacked the research background. It presents the research problem, aim and objectives of this study, as well as research questions. This chapter also discusses the significance of the study.

CHAPTER 2: LITERATURE REVIEW

Chapter two defines the concept used in this research. It intensely discusses the literature in the context of cyber-loafing activities and challenges in the workplace. This chapter also presents literature on the tools used by managers to control cyber-loafing activities. Furthermore, the theoretical frameworks that were employed in this study and the research gap are presented in this chapter.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter provides an overview and discussion of the research design and methodology adopted in this study. Moreover, it details the specific methods used to collect and analyse empirical data. This chapter also explains how the issues of reliability, validity and ethics were addressed.

CHAPTER 4: FINDINGS, DISCUSSION, AND INTERPRETATION OF FINDINGS

This chapter presents the research findings from the literature and empirical study. The discussion of the research findings is structured such that it addresses each research objective.

Chapter 5: Recommendations and Conclusion

This last chapter summarises the research and its findings. The objectives and questions of the research are revisited and then the conclusion and recommendations are presented in this chapter.

1.8 CONCLUSION

The introduction and background to the study set the tone for this study. discussed in this chapter. Managers lack the necessary skills and tactics for reducing workplace cyber-loafing, according to research. The chapter provides a literature review on the evaluation of tools used by managers to prevent and control cyber-loafing by the administrative staff in the case study of eThekwini Municipality Sizakala Customer Care.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter presents explanations for the terms that were used throughout this study. It elaborates on cyber-loafing, making inferences on studies that were previously conducted on the subject, with a deeper focus on the roles that managers of organisations play in mitigating cyber-loafing behaviour among members of staff. In addition, it evaluates the strategies that can be applied to assist managers in reducing the rate of cyber-loafing while also suggesting novel measures to mitigate this behaviour among workers. The chapter concludes with a discussion of factors that positive affect the implementation of tools that can be used by management to control cyber-loafing by their subordinates.

2.2 OPERATIONAL DEFINITION

As a point of departure, the key term used in this study is defined below as follows:

- **Cyber-loafing**

The term cyber-loafing was first used by Kamins in 1995 (Aku 2017: 25; Elciyar and Simsek 2021: 44). Cyber-loafing is described as intentional or voluntary activities by employees during working hours, using the company's internet and computer resources for personal activities or activities that are not related to their official assignments hence neglecting their duties (Jandaghi *et al*. 2015: 46). According to Jandaghi *et al.* (2015: 55), the term cyber-loafing is a combination of two words. Loafing comes from the word loafer referring to a person who misuses his or her time. The word cyber, on the other hand, is an adjective that describes anything related to computers, information technology, the Internet and virtual reality. Hence, cyber-loafing refers to a behaviour whereby a person wastes time performing computer and internet-related duties (Jandaghi *et al.*

2015: 55). The aforementioned authors further explain the term as when a person purposely engages in the usage of their organisation's internet access to engage in non-work-related duties during work hours which do not require too many technological skills. This act negatively affects the organisation, as employees who engage in cyber-loafing are likely to produce work of poor quality and a reduced quantity, which degrades the work outcomes and standards (Jandaghi *et al.,* 2015: 56).

2.3 CYBER-LOAFING CHALLENGES IN THE WORKPLACE

To have a better insight into the cyber-loafing challenges in the workplace, it is pivotal, to begin with the discourse on the types and categories of cyber-loafing.

2.3.1 Cyber-loafing categorisation and typology

Cyber-loafing is divided into two components, which are browsing and emails (Cook 2017: 55). Browsing actions involve visiting websites for entertainment, financial services, news, social networking, shopping, sports and pornography. Emailing involves receiving and sending emails for personal purposes using a company computer and the Internet (Kasap 2019: 55). Another type of cyber-loafing involves interactive internet activity. Interactive cyber-loafing is when individuals play live online games, chat online, make live posts on social networking sites and download information (Aku 2017: 56).

Cyber-loafing is further categorised into minor and serious cyber-loafing based on the severity of the deviant behaviour (Elciyar and Simsek 2021: 17). The cyber-loafing typology was developed based on the device or computer in the workplace (Kaptangil 2021: 44). Various communication tools can be linked to cyber-loafing. Smartphones, smartwatches and tablets are part of the communication technologies that enable users to access cyberspace. It is important to note that employees do not only need to work on computers to engage in cyber-loafing activities; they can use their personal devices to connect to their company's Wi-Fi and engage in cyber-loafing activities.

Cyber-loafing behaviour can be divided into four categories based on the underlying behavioural intent (Radebe 2020: 47). These include classifying cyber-loafing as a development behaviour, recovery behaviour, addiction behaviour, or deviant behaviour (Kasap 2019: 35; Malik Saleh 2018: 18; Şİmşek and Şİmşek 2019: 36). When cyber-loafing harms an individual's job performance and poses negative effects on organisational performance and productivity, it is considered deviant behaviour. Cyber-loafing is considered an additional behaviour when an individual who is suffering from internet addiction in their personal life may also have problems with their work life regarding interpersonal relationships and productivity.

Cyber-loafing activities that occur due to employee addiction to the Internet are categorised as addictive behaviours (Toker and Baturay 2021:45). From an organisational perspective, this act is not acceptable as it neutralises employees' work satisfaction and mental health in a negative way (Li 2017: 25). Finally, cyber-loafing behaviour can be considered a development tool if employees use the Internet to learn new things to improve their work conditions (Kaptangil 2021: 56). Employers can benefit from such activities by developing their innovative skills and enhancing their working abilities, not to mention the positive impact they have on an organisation. In such a case, cyber-loafing is considered to be a development performance (Abbasi 2018: 24).

For the organisation to evaluate control measures, it is important to distinguish the two types of cyber-loafing based on the severity of the cyber-loafing deeds. These are minor, not severe or extreme cyber-loafing behaviours (Jandaghi *et al.* 2015: 44). Minor or not severe cyber-loafing activities range from sending or receiving personal emails using the company internet and computer during working hours to reading news on the Internet. On the other hand, actions that are considered to be extreme or severe cyber-loafing include playing games, accessing adult websites, logging on to social media, internet banking, shopping online, job searching, downloading non-work-related and personal stuff and gambling online (Jandaghi *et al.* 2015:25) and Elciyar and Simsek (2021: 56).

Although certain activities are generally perceived as severe or extreme cyber-loafing actions, for example, playing online games and viewing adult websites, cultural perceptions and values are significant determinants in the categorisation of cyber-loafing activities (Sage 2015: 23). Organisations must understand and separate these two types of cyber-loafing to establish appropriate tools for each category and develop measures for controlling or mitigating such behaviour among their employees.

2.3.2 Employees' Participation in Cyber-Loafing

In recent years, the use of internet technology has increased in the workplace to improve employee performance. Cyber-loafing is considered a workplace deviant that affects employees' performance and efficiency (Dmour *et al*. 2019: 45; Hadlington and Parsons 2017: 44; Khansa*,* Barkhi, Ray and Davis. 2018: 34). It has been noted that male employees are predisposed to higher cyber-loafing behaviours than female employees (Malik 2018: 31). Cyber-loafing can cause serious damage to the company; employees who perceive themselves as powerless in their work environment are likely to engage in cyber-loafing activities. Job satisfaction and organisational justice have been identified as major influences or motives of cyber-loafing in an organisation (Malik 2018: 33).

An employee's cyber-loafing activities do not depend only on psychological factors but also on other factors like organisational factors, for example, the work environment and personal ones like the individual needs of the employees (Kaptangil 2021: 26). An employee who engages in cyber-loafing behaviour not only negatively impacts their organisation financially but also tends to compromise job quality, which violates the expected job standards (Elciyar and Simsek 2021: 69). Furthermore, it wastes employees' time, which results in a substantial loss of organisational productivity.

Khansa *et al.* (2018: 34) state that the loss due to these activities comes in the form of annual costs for the organisation due to security violations, viruses, lower

job productivity, identity and information theft, hacking, time-wasting and nonworking internet usage and that this represents a significant loss to companies and organisations. There are direct and indirect costs associated with cyber-loafing (Elciyar and Simsek 2021: 17). Indirect costs result from procedures and actions that destroy brand images, thus leading to loss of customer loyalty and customers losing trust in the organisation (Dooly 2021: 58). Many companies do not report cyber-loafing incidents that occur at their work environment that increase the organisational costs. (Abbasi 2018: 24).

Recent studies indicate that organisations have begun to legalise the use of monitoring systems in the workplace to curb cyber-loafing activities (Kwon 2015: 28). For the organisation to control or determine which strategy works effectively, managers of organisations must have a clear understanding of the cyber-loafing phenomenon. As claimed by Kasap (2019: 36), the majority of employees use their company's internet to browse non-work-related websites and the majority of these individuals send and receive personal emails at the workplace during working hours.

It is estimated that employees spend two to three hours a week cyber-loafing, which is equivalent to half an hour a day. A large number of employees engage in cyber-loafing activities to perform their duties, such as news, social media, online shopping, entertainment and lifestyle, sports and travel (Kasap 2019: 33). The severity of cyber-loafing behaviour differs from person to person. Some individuals may use the Internet excessively for work purposes, and some may abuse the opportunity for shopping, personal communication, playing a game, or personal business purposes during the time that is allocated for work purposes (Ozdamli and Ercag 2021: 39).

2.3.3 Consequences of Cyber-Loafing

After highlighting the challenges organisations face due to cyber-loafing activities, this section highlights the negative impact and damages that this phenomenon

may have on the organisation. The consequences of cyber-loafing can be attributed to the nature of its impacts, that is, whether it has positive or negative impacts (Holguin and Emilsen 2016: 59). When it has negative implications for the organisation, such as cost and loss of productive time and reduced job performance, it is destructive. In contrast, when cyber-loafing behaviours have a positive outcome for the organisation, which can lead to increased job productivity, innovation and creative work behaviours, job satisfaction, it is constructive (Kaptangil 2021: 14).

The consequences of cyber-loafing may be investigated from an individual and organisational perspective (Abbasi 2018: 33). From an individual perspective, destructive cyber-loafing behaviours may consume productive time, distract employees from their official duties and reduce work efficiency and task performance (Khansa, *et al*. 2017: 39). Cyber-loafing may pose severe and dangerous consequences for the employee, including loss of life. Mercado *et al. (*2017:29) reported the case of an inattentive train dispatcher who failed to direct two trains properly while playing mobile games on the job. When employees engage in cyber-loafing activities as a recovery or stress coping mechanism, this can improve their work performance since they can recover from job-related physical or mental fatigue (Fezile Ozdamli 2021: 25).

The issue of job performance concerning cyber-loafing has been deeply investigated. Studies agree that minimal cyber-loafing can create better morale and act as a recreational activity. On the other hand, a high level of cyber-loafing can be exhausting for the employee and can lead to inefficiency (Jandaghi 2015: 96; Kasap 2019: 68). When employees engage in non-work-related browsing on the Internet, some information garnered during such activity may be valuable to improving employee knowledge and a better understanding of their work. In addition, the use of social media platforms may promote employees' social capital, thereby facilitating knowledge transfer and consequently, improving work performance (Mercado *et al.* 2017: 59).

From an organisational perspective, destructive cyber-loafing behaviours, such as the misuse of email services, use of adult websites and online gambling, downloading illegal software and accessing unauthorised information may threaten organisations' legitimacy and lead to liability, data security and confidentiality breaches (Kasap 2019: 66). All these factors can lead to legal issues and increased costs for the organisation (Kasap 2019: 109; Hadlington and Parsons 2017: 45). A study by Hadlington and Parsons (2017: 11) highlighted the risks associated with destructive cyber-loafing, such as the propensity to visit adult websites, online gambling and company information security breaches Jandaghi *et al*. (2015: 36) noted that organisations incur billions of US dollars in costs due to losses in productivity, security and internet-related incidents, legal actions and other associated costs.

Lost productivity and reduced job performance are important consequences that organisations suffer because of cyber-loafing behaviours among workers. Engaging in cyber-loafing, requires cognitive skills, energy, time and attention, which becomes very difficult for the employee to switch back to their work duties (Dooly 2021: 39). In extreme cases of cyber-loafing, employees procrastinate and mostly postpone their tasks; hence, timely completion of tasks is not achieved which can lead to poor organisational performance (Sage 2015: 49).

In the previous section, some of the activities that pertain to cyber-loafing have been highlighted**.** Table 2.1 is a list of cyber-loafing activities as well as the authors.

Table 2. 1 Common cyber-loafing activities in the workplace

Cyber-loafing Behaviours	**Researchers**
Online shopping	Coker, 2011; Hassan *et al.* 2015; Sheikh, *et al*. 2015; Ugrin and Pearson, 2013
Money management	Coker, 2011; Hassan *et al.* 2015; Sheikh *et al.* 2015; Ugrin and Pearson, 2013;
Social networking	Coker, 2011; Hassan *et al.* 2015; Karaoğlan *et al*. 2015; Sheikh *et al*. 2015; Ugrin and Pearson, 2013;
Adults' websites perusal	Coker, 2011; Hassan *et al*, 2015; Ugrin and Pearson, 2013
Emailing (other than work emails)	Lim and Chen, 2012; Coker, 2011; Sheikh *et al*. 2015; Hassan *et al* 2015; Ugrin and Pearson, 2013;
Web browsing (e.g., lottery, news, sports; auctions, gaming)	Coker, 2011; Sheikh *et al*. 2015; Hassan *et al*. 2015
Streaming media	Ugrin and Pearson, 2013; Coker, 2011; Hassan *et al*. 2015

2.4 TOOLS USED BY MANAGERS TO CONTROL CYBER-LOAFING ACTIVITIES

Since cyber-loafing negatively impacts employee performance and productivity, organisations have a huge responsibility to control and reduce this behaviour. While organisations have adopted various forms of technical deterrence mechanisms, cyber-loafing continues to increase. The role of the manager in mitigating this behaviour by employees is not clear, hence the need to evaluate and review the existing cyber-loafing mitigation tools and strategies.

The general deterrence theory (GDT) was adopted to investigate and explain possible mechanisms and strategies for preventing and mitigating cyber-loafing

activities among employees. This theory is based on an imposed regulatory model and emphasises regulatory principles imposed by organisations on their employees through the threat of sanctioning (Song 2021: 20). GDT, as shown in Figure 2.1, consists of three categories that influence legal behaviour: sanctions, detection and enforcement. Furthermore, this theory is based on the idea that human behaviour is rational to a degree and may be influenced by incentives, particularly negative incentives, such as those found in formal punishments (Song *et al.* 2021: 20).

When the possible penalty is weighed against the potential reward of engaging in particular activities, the prospect of retribution, according to GDT, may have a substantial impact on employee intentions and actions (Song 2021: 67). GDT has been widely used to explore and explain processes that are aimed at lowering employee participation in unproductive workplace deeds such as cyber-loafing (Song 2021: 67).

GDT is most commonly used in criminal justice, ethics and, more recently, cyber-loafing (Li 2017: 36). It proposes a system in which the consequences of improper behaviour are fully specified, revealed and punished as a result of qualified discovery methods. According to the GDT, two types of cyber-loafing mitigation strategies that seem to lower cyber-loafing activities are the use of workplace internet policies and electronic monitoring systems (Hassan, Reza and Farkhad 2015:33). Using GDT, Ugrin and Pearson (2013), evaluated the effectiveness of appropriate use policies and electronic monitoring in curbing cyber-loafing in the workplace. According to (Song 2021: 67), individuals tend to act accordingly if the punishment is extreme compared to the benefits derived from the individual's actions. Some scholars discovered that there is a relationship between the effectiveness of deterrence and method and individual characteristics.

Ugrin and Pearson (2013) noted that deterrence mechanisms such as threats of sanctions and termination of employment were effective in preventing some types of cyber-loafing activities. The organisation needs to properly explain to its

workers the detrimental effects of cyber-loafing. Awareness among employees of the implications of cyber-loafing on company information security can be used as a tool to mitigate cyber-loafing activities in the workplace (Hadlington and Parsons 2017: 44). However, findings from Saleh *et al.* (2018: 35) indicate that the certainty of detection and threat of sanctions and punishments lead individuals to hide their cyber-loafing activities. Due to this, employees prefer to use their smartphones when engaging in cyber-loafing, especially when they are sure of being detected by company monitoring systems.

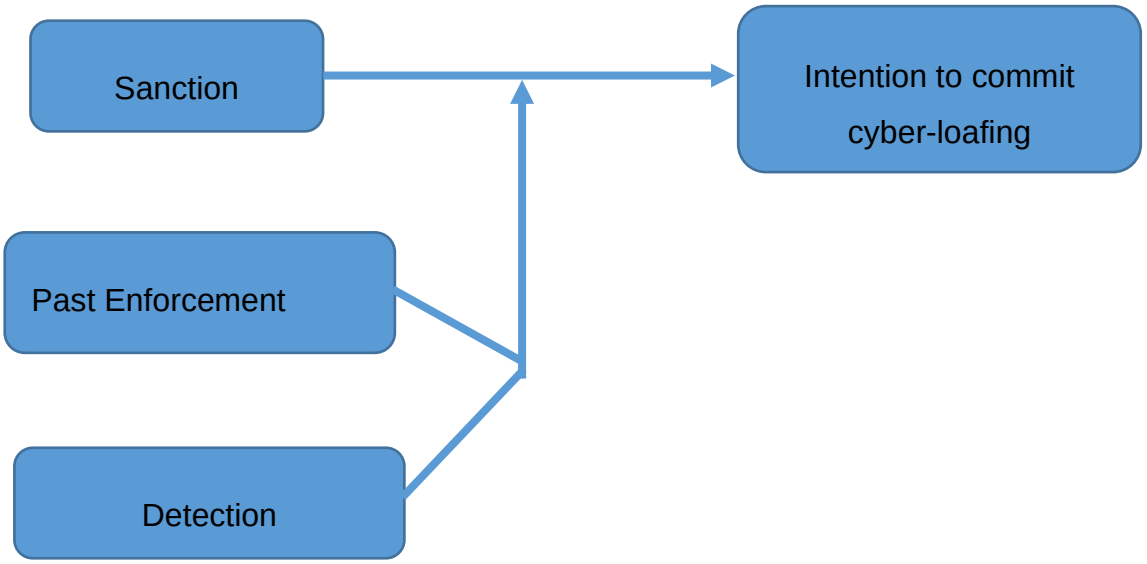


Figure 2. 1 Deterrence model in cyber-loafing

Source: Ugrin and Pearson (2013)

- **Sanctions**

The sanctioning component of the GDT model is crucial for Individuals' trust in the scope. The severity of the promised consequences is a deciding factor in whether or not they engage in undesirable behaviour, such as cyber-loafing (Hassan *et al.* 2015: 19). In other words, the likelihood of the promised penalties occurring is a major deciding factor in deterring employees from engaging in cyber-loafing activities (Hassan *et al.* 2015: 19; Song, Ugrin, Li, Wu, Guo and

Zhang 2021: 20). For penalties or punishments to be effective as deterrents, they must be immediate and likeable (Song 2021: 20).

Furthermore, from the standpoint of cyber-loafing, organisations that impose more punishments are more likely to have a low number of people involved in cyber-loafing (Hassan *et al.* 2015: 19). When a business has punishments in place, employees are less likely to engage in cyber-loafing. People tend to avoid doing what would cause them to break the law or become offenders, according to this idea, when substantial costs and repercussions are associated with their actions. For example, the availability of suitable punishments and knowledge of previous enforcement.

The use of deterrence as a technique for reducing the high rates of cyber-loafing among employees has been criticised for its many flaws. Threats of legal punishment, for example, have been related to a rise in Internet abuse. Furthermore, social norms and observability were said to have a significant impact on the effectiveness of deterrence in reducing employee cyber-loafing (Song *et al.* 2021: 24). However, the perceived certainty and severity of possible cyber-loafing punishments were found to mitigate the impact of observability on employee cyber-loafing. The threat of punishment was almost ineffective at curbing cyber-loafing behaviour among employees due to earlier experience or the possibility of punishment avoidance (Hensel and Kacprzak 2021: 36).

- **Detection and past enforcement**

The effect of possible fines on cyber-loafing will be tempered by an increased chance of discovery and evidence of prior enforcement for less abusive manners, according to Ugrin and Michael (2013: 02). This indicates that employees who are aware of formal detection methods are less likely to engage in cyber-loafing operations.

- **Severity of Sanctions**

Determining whether the certainty or severity of punishments deters offenders from engaging in rebellious conduct is a contentious issue. With actual data on

both sides of the debate, this facet of the deterrence concept has been demonstrated to have a major influence on the deployment of deterrent techniques to limit cyber-loafing activities. According to Ezeh, Etodike, Chukwuemeka and Emmanuel (2018: 45), the severity of sanctions is more important than the certainty of punishment. Employee perceptions of the severity of punishments have a negative influence on employee intention to misuse the organisation's internet resources, according with Song *et al* (2021: 45), whereas this is not seen for workers' perceived certainty of sanctions.

Similarly, Radebe (2020: 46) found that workers' intentions to break their organisation's internet service security policy were influenced by the perceived severity of punishments, but the perceived certainty of sanctions had no statistically significant effect. In contrast to the foregoing, empirical data suggests that the certainty of punishment, rather than the harshness of sanctions, deters workers from engaging in a rebellious manner such as cyber-loafing. Employees from various organisations had a statistically significant influence on their desire to comply based on the certainty of discovery (Song *et al*. 2021: 45).

Tools that are commonly used by managers to control cyber-loafing are highlighted below as follows:

2.4.1 Policies

Policies that are well-written will encourage positive usage while limiting activities like cyber-loafing (Kim 2018: 55). Policies promote information flow and boost production (Galli 2015: 06). Users will be able to comprehend and work within the policies' expectations. When diverse parties work together to design and change policies, it increases cooperation and promotes common understanding (Galli 2015: 41; Kim 2018: 44). However, a badly drafted or administered policy might have detrimental consequences. When it comes to preventing cyber-loafing, a poorly worded policy might be damaging. Overly restrictive policies can hinder

innovation and collaboration (Galli 2015: 23). Poorly worded regulations create ambiguity, which appears to allow cyber-loafing

Despite regulation, certain employees will be more prone to engage in cyber-loafing. Human nature appears to look for loopholes. Employees may, for example, shift their cyber-loafing activities to their mobile phones or personal computers to get around a policy that solely applies to corporate resources. Kim (2018: 28) points out that policies should be detailed enough that employees cannot identify loopholes. The policy must be supported by management. Support entails active engagement and involvement in policy creation and implementation (Mohammad *et al.* 2019: 44). Employee and management collaboration in policy formulation results in a feeling of trust, which leads to higher levels of obedience (Kim 2018: 66). A good policy is physically sound, with any negative effects taken into account (Jiang *et al.* 2020: 54).

2.4.2 Electronic Monitoring Systems

Within an organisation, monitoring is a major technique for managing cyber-loafing habits. Monitoring, in particular, inhibits non-work-related internet usage (Gorenc *et al.* 2016: 16). Monitoring software keeps track of how much time employees spend on corporate computers doing things that are not work-related (Arciniega *et al.* 2017: 36). The programme keeps track of browser history, keystrokes and websites one visits (Gorenc *et al*. 2016: 26). Unauthorised internet activity may be tracked by recording keystrokes, which can be used as a cause to monitor internet activity. Employee computer usage is monitored for a variety of reasons, but one of the most common is to prevent danger. According to one of the first publications on cyber-loafing, it is important to monitor cyber-loafing for several reasons, including preserving productivity, preventing infections, maintaining security, preventing the company's network from being exposed, preventing corporate espionage, and avoiding financial hazards (Kim 2018: 59).

Regardless of the safeguards in place, certain workers are still found to cyber loaf. Monitoring will not discourage this type of activity among these workers (Arciniega *et al.* 2017: 56). Others regard cyber-loafing, or at the very least the knowledge obtained while on the Internet for personal purposes, as a kind of self-improvement (Arciniega *et al*. 2017: 55). Part of the problem is that as people have become more connected, the lines between work and personal time have blurred (Hagqvist *et al.* 2020: 66). Why not check personal email at work if users check work email at home? Monitoring, on the other hand, may be beneficial to some employees. Formal measures, such as monitoring, can help to decrease the purpose of cyber-loafing (Khansa *et al*. 2017: 56). One technique that may decrease cyber-loafing is policy confirmation via monitoring software (Arciniega *et al.* 2017: 36). Another helpful regulation is formal instruction on the proper phone, internet and other communication usages (Gorenc *et al.* 2016: 55). Another formal control is the use of quota modules, which allow for some personal use while alerting the user when the quota is reached (Jeong *et al*. 2020: 56).

2.4.3 Managerial Control

Managers must promote adherence to the cyber-loafing policy. Compliance can be improved by ensuring staff understand why the practice is beneficial to the company's success (Curry *et al.* 2017: 28). Employees, regardless of the company, are resistant to change owing to disturbances in their routine or even fear of instability Galli (2015: 66). A forced alteration may be perceived as an injustice by employees. Some may use cyber-loafing as a tool to overturn a perceived injustice due to an aversion to change (Akbulut *et al*. 2017: 44). When there is respect and confidence in management, change is more likely to be embraced (Veridiana *et al.* 2019: 56). Employees must be able to manage change to comprehend and follow rules and processes that decrease cyber-loafing. When utilised within the organisation's rules, communication tools like cell phones and email boost productivity (Hassan *et al*. 2017: 27). Computer abuse is reduced

by using codes of conduct in combination with written policies (Jafarkarimi *et al*. 2016: 45). Rules and procedures based on governance structures after they have been created and defined should be established by management.

2.4.4 Other deterrent mechanisms

- **Organisational Control Mechanisms**

Organisational control is closely associated with managerial control, system control, policy control and behaviour control. This describes the laid-down procedures that an organisation uses to control employees' activities and engage them to ensure compliance with the organisation's policies and goals (Abbasi 2018: 105; Piscotty et al. 2016: 66). It involves the application of rules and policies, legitimate authority, standards, any written documentation and other control measures in a bid to control and standardise employee attitude and performance (Kasap 2019: 24). Employees will follow rules and policies enforced by managers in the workplace if they realize they will be punished if they do not adhere to them

Once employees understand that there are punishment protocols in place for violating organisational policies, they will refrain from committing such unacceptable and deviant behaviour (Saleh *et al.* 2018: 55). An employee's conduct can be controlled and minimised by the manager if they believe they are receiving formal punishment if they are cyber-loafing during working hours. Companies need to develop and implement effective strategies to control cyber-loafing in a work environment that uses controlling and punishment tactics to reduce cyber-loafing actions. It is also crucial that supervisors monitor their employees, understand their cyber-loafing manner in-depth and enforce punishments if any violations take place (Khansa *et al*. 2017: 56).

- **Prevention Strategy**

Prevention policies are strategies that are targeted at minimising employee violations of company policies. Preventative technology may also assist the organisation to grow its business, but the abuse of technology in an organisation can lead to organisations losing their reputation and customers (Kwon 2015:44). Managers of organisations are required to implement an effective prevention strategy. The first rule is to ensure the adopted organisational online policy includes unambiguous points that are linked to the organisation's rules and policies (Glassman *et al.* 2015: 105). Training and educating employees about potential security risks and negative consequences and creating awareness about their responsibilities are important alternative management practices in organisations that can serve as a preventative strategy for curbing cyber-loafing practices among employees (Dooly 2021: 45).

Recent observations by Hadlington and Parsons (2017: 106) highlight a strong positive link between indulgence in severe cyber-loafing activities and poor internet security awareness. Supervisors and managers need to be trained on security concepts so that when they advise employees, they do so with the requisite understanding of the risks that employees may face by violating organisation policy (Cook 2017: 55). Junior employees need to get training as well with regards to security violation policies before they can comprehend the risks involved in committing such an act in the workplace (Li 2017: 45).

2.5 FACTOR AFFECTING SUCCESSFUL IMPLEMENTATION OF CYBER-LOAFING MANAGEMENT TOOLS

Although tools to prevent cyber-loafing have been identified and discussed, more research into what influences their implementation is needed. Particularly considering the rapid increase of cyber-loafing among employees, as already discussed in the above section. Factors affecting the successful implementation of cyber-loafing management tools include:

2.5.1 Habit and Belief

The term "habit and belief" refers to situational behavioural patterns that happen automatically without the need for conscious decision-making to respond to specific cues (Triandis, 1980). Once a habit is developed, cyber-loafing is routinely carried out without conscious effort or consideration of the consequences. In other words, when a student has a strong habit and belief in cyber-loafing, the influence of their intention to cyber-loaf is diminished, indicating that they may no longer need to assess their attitudes and subjective norms before engaging in cyber-loafing conduct (Askew *et al.* 2014: 56). By completing repetitive activities mindlessly and without considering the repercussions, many workers develop the habit of cyber-loafing (Koay and Soh 2018: 68). Employees regularly engage in cyber-loafing while at work since habits may shape a person's behaviour and lifestyle once they become established (Dmour *et al.* 2020: 69).

2.5.2 Daily Workload

A daily workload is the quantity of work that is seen to be engaged in terms of complexity, volume and speed, according to certain research. Alarcon, Bragg and Hartman (2015: 36) assert that high workloads are bad for both workers' and companies' productivity. The meta-analysis by Mercado *et al*. (2017: 56) found that it is disappointing that businesses are placing more responsibility on non-work-related activities since this workload would hurt output and cause losses for the organisation.

Dmour *et al.* (2020: 86) conducted an investigation of Facebook usage at workstations at a company in 2013. To evaluate the workload literature with objectivity, Bowling *et al.* (2015: 68) used meta-analysis to examine potential correlations and effects of workload. Employees were more prone to cyber-loaf if they were bored than when they were overworked (Carnevale *et al.* 2020: 56). To put it another way, staff workers may use cyber-loafing as a coping mechanism for boredom and underloading. Managers who supervise employees in

occupations that experience underload may assist subordinates in developing productive coping mechanisms by offering exciting tasks or engaging in developmental activities that would keep workers focused on their job and away from their electronic devices (Sampat and Basu 2017: 54).

2.5.2 Virtual Work

In certain sectors, business owners choose a virtual work space for their company due to excessive costs and unsuitable workspaces. Employees can work remotely without regard to location by using the concept of virtual work space. The idea itself and its principles are gaining popularity due companies should cut costs and improve workplace flexibility. However, it has been discovered that when employees have less oversight, they are more likely to indulge in online gaming while working virtually (Dmour *et al.* 2020: 86). However, COVID-19 has abruptly altered everyone's world. Lockdowns shocked people, cities, economies, nations and continents and the fear of uncertainty gripped them all. In a short period, managers had to decide several things, including who should stay at work and who should go, how and where individuals should migrate into the digital world, what their objectives are and how to effectively communicate those values to their staff.

Both social and commercial life have undergone significant alterations and modifications as a result of the COVID-19 epidemic, which has now become a worldwide calamity (Kasap 2019: 24). The escalating global crisis has made it necessary (rather than an option) to move procedures to digital platforms as organisations prepare to adapt to technology-based processes (Kaptangil 2021: 44). As a result, corporate practices and workplace culture have altered and the shift to flexible work models, particularly remote work, has started. Instead of happening gradually, this transformation happened fairly quickly.

Through this approach, employees may now debate new concepts and hazards as well as raise awareness of current concepts and risks, which has established

a new normal in the workplace. Since the COVID-19 outbreak, several firms have updated their plans, projections and courses of action based on risk assessments. Business managers now need to manage the process as precisely and successfully as possible and be more solution-oriented than before. In any aspect of life, but notably in the business world, decisions that are put into action as solutions can develop into issues over time and every solution starts to show signs of difficulties.

Employers and workers alike must become accustomed to working remotely without the choice of other workspaces (Carnevale *et al.* 2020: 56). In this scenario, the distinction between work and family is becoming increasingly hazy as homes are converted from living to working areas. With the shift to home/work policies following COVID-19, the need for technical control measures created to counteract the cyber-loafing the inclination of employees to use email and the Internet for personal purposes while at work has expanded abruptly and severely. Employers use technology solutions as a method to reduce waste in a volatile and unpredictable environment to increase company performance and efficiency through controlling operations (Hensel and Kacprzak 2021: 36).

Investments in remote working technology also appear to make sense in the post-COVID-19 era. For businesses that wish to migrate production online while keeping the ability to closely monitor staff's actions, the International Journal of Contemporary Management offers a ready-made, turnkey solution (Song *et al*. 2021: 45). How we respond to a life crisis centred on fundamental issues of life will be determined by the development of a technology-driven future and the process that emerges alongside the pandemic, known as the new normal.

These issues include what we believe, how we think, how we visualise our role in life, what our next generation's core elements are, what emotions, thoughts and behaviours we feel and exhibit, and how uncertainties about individual and corporate decisions can be resolved, and what solutions are impending. The

negative behaviours that existed before the new normal may be reclassified as good ones (Dooly 2021: 45). By developing the practice of working remotely, it would even be possible to promote them as tools to avert fresh life crises for both institutions and workers. Some characteristics are shared by effective technology usage policies.

The policy must be supported by management. Support entails taking an active role in the formulation of policies and ensuring their observance (Mohammad *et al*. 2019: 89). Support includes educating staff members on the importance of the policy (Jiang *et al.* 2020: 104). Cooperation in policy formulation between management and employees fosters trust, which improves compliance (Kim 2018: 106). A sound policy weighs possible negative impacts while being structurally sound (Jiang *et al*. 2020: 105). However, there should be considerable leeway in the formulation of policies and in identifying the necessity of editing as new. Situations occur (Sampat and Basu 2017: 54). Although Kim (2018) observes that policies should be sufficiently detailed so that employees cannot identify exceptions, Galli (2015: 36) contends that rigidity can encourage cyber-loafing.

2.5.3 Workplace Conditions

Open environment and academic freedom: If an assault takes place in an open setting, it is challenging to monitor the information system. Additionally, it is challenging to reduce the hazards and choose the ideal remedy for cyber-loafing. a lack of funds Organisational executives may disregard the value of having a security system due to the high expense of security technologies. This is especially true if they are unaware of the true worth of these systems, the losses they would incur and the negative effects that ignoring them will have on the business. Security is just second in importance. Security is frequently ranked low on the priority list by corporate executives, particularly when they outsource services or work with outside contractors. Organisational leaders must prioritise

security in their plans to lessen cyber-loafing activities. If there is a flaw in security services or security software, sanctions should be established.

Every organisation has a unique policy and each has different security guidelines. When organisations integrate or merge with other organisations or when there are security discrepancies, conflicting security regulations and policies may develop. technical difficulties. Because of the complexity of system technology and the organisation's networks, it is challenging for vendors to comprehend the requirements or demands of organisations (Li 2017: 45). Networks inside an enterprise may employ a variety of technologies to control access to network components, including routers, switches and firewalls, as well as to manage the data system.

2.5.4 Organisational Culture

Studies show that norms that support cyber-loafing among co-workers and supervisors are positively connected with it. This shows that there is a good chance of normative control over cyber-loafing (Jafarkarimi et al. 2016: 45). Employees should turn to their co-workers as potential role models in the workplace since, according to (Radebe 2020: 47), cyber-loafing is learned by emulating the behaviours that others in their corporate context show (Khansa 2017: 54). People use the normative environment as justification for acting in ways that their peers do (Lim and Tee 2005). People were more inclined to engage in these actions themselves if they were aware that their co-workers also displayed comparable tendencies (Hadlington and Parsons 2017: 45).

2.5.5 Organisational Policies

When attempting to reduce cyber-loafing, a poorly designed policy might be damaging. Too strict rules can impede innovation and collaboration (Galli 2015: 69). Despite the rules, certain employees will be more prone to indulge in cyber-loafing (Arciniega *et al*. 2017: 54). Policies that are poorly stated lack clarity,

which seems to allow for cyber-loafing It is human nature to look for loopholes. Employees may, for instance, switch their online activity from desktops to mobile devices to circumvent a rule that solely applies to business resources. 7Small firms must be able to create effective policy action systems since inadequately formulated policies are a problem.

Clear Internet usage guidelines should be developed and implemented by managers to reduce the detrimental consequences of cyber-loafing while maintaining the positive ones (Werner 2020: 76). A clear Internet policy that warns of the potential consequences may reduce employees' inclination to abuse the Internet (Kaptangil 2021: 21). Several characteristics are shared by effective technology usage policies. The policy must be supported by management. Support entails taking an active role in the formulation of policies and ensuring their observance (Mohammad *et al.* 2019: 67). Support includes educating staff members on the importance of the policy (Jiang *et al*. 2020: 68). Cooperation in policy formulation between management and employees fosters trust, which improves compliance (Kim 2018: 126). A sound policy weighs possible negative impacts while being structurally sound (Jiang *et al.* 2020: 69). However, policy formulation must be flexible and acknowledge the need for revision when new circumstances occur (Sampat and Basu 2017: 66). Gallini (2015: 39) contends that rigidity can promote cyber-loafing; however, Kim (2018: 56) points out that regulation should be sufficiently detailed so that employees cannot identify exceptions.

2.5.6 Training and Education

No plan can be effective unless it is effectively implemented and maintained to raise value awareness or perception (Dooly 2021: 56). With an understanding of the consequences of the activity, habit strength declines. This indicates that some degree of self-control may be restored by just informing people about the extent of their involvement in the repeated activity and linking it to potentially negative outcomes, such as missed deadlines and subpar employee ratings (Issock and

Mpinganjira 2020: 45). Training also improves compliance. Employees are empowered by policy training as they become more aware of internet abuse and its expensive impacts on the company (Hadlington and Parsons 2017: 45). Some workers continue to disregard the cyber-loafing policy.

2.6 THEORETICAL FRAMEWORK

Identification of cyber-loafing that is common amongst organisations was achieved by using the five-factor model of personality and the theory of interpersonal behaviour (TIB). Literature has linked cyber-loafing activities with these theories (J-Ho and Ramayah 2017: 75; Sage 2015: 78; Lee and Ohtake 2018: 28).

2.6.1 Five-factor model of personality

Sage (2015: 76) developed the five-factor model of personality, which is used to characterise workplace personality features because it is a helpful tool for assessing distinct personality qualities that are linked to a range of professional actions (Dooly 2021: 107). This personality model has a lot of applications in the workplace (Khansa 2017: 59) and it is a great way to assess distinct personality traits that are linked to a range of professional manners. The five-factor model is a collection of personality characteristics that indicate stable individual variations in people's ideas, feelings and deeds (Sanaullah *et al.* 2021: 20). The main categories of the model are extraversion (surgency), agreeableness, conscientiousness, emotional stability (neuroticism) and openness to experience.

Extraversion (Surgency): This refers to a person's proclivity to be aggressive, social, outspoken, active and vivacious, as well as to feel good emotions and think positively (Sanaullah *et al*. 2021: 27). Extroverted people are active and work well with others, according to. Introverted people, on the other hand, are less socially active and more restrained in social circumstances (Sage 2015: 65).

Agreeableness: This reflects a person's level of cooperation, selflessness and trustworthiness (Sanaullah *et al.* 2021: 44). Agreeableness is also said to refer to how well one gets along with others and it encompasses traits such as altruism, trust, warmth, prosocial and empathy. People who have a low level of agreeableness are often hostile, self-centred, spiteful, or resentful toward others (Sage 2015: 33).

Conscientiousness: Individuals that are self-disciplined, dependable, committed, responsible, loyal, achievement-oriented, organised and diligent are credited with conscientiousness(Blanchard 2019: 67). Conscientiousness also refers to a disciplined pursuit of predetermined objectives and a tight commitment to predetermined or personal ideals. Individuals who score lower on this behavioural trait are more likely to be unproductive, unmotivated to achieve and disorganised in general. Conscientious people usually go above and beyond what is required of them since they are highly driven (Kwon 2015: 07).

Neuroticism (Emotional Stability): This personality trait appears to be the direct opposite of extroversion. Neurotic individuals tend to experience negative emotions (for example, anger, anxiety, depression and sadness) and are predisposed to negative thoughts (for example guilt, self-doubt and worry). Neuroticism generally represents the predisposition to experience psychological distress. Individuals who score low on emotional stability tend to experience bad emotions, such as stress, anger, or depression (Barlow *et al.* 2014). Their chronic pattern of extreme worrying, instability, self-consciousness and low-stress tolerance makes them suffer from psychiatric disorders (Li 2017: 07). In contrast, individuals who score highly in emotional stability tend to be calm, relaxed and steady (Sage 2015: 111).

Openness to experience: This personality attribute is defined by a shared enthusiasm for art, adventure, unusual ideas and inventiveness, imagination, aesthetic sensitivity, curiosity and a desire to broaden one's horizons (Sage 2015:44; Chen *et al* 2017: 15). People who are open to experience are

intellectually curious, open to emotion, sensitive to beauty and non-dogmatic (Sage 2015: 44). They are more inventive and conscious of their sentiments when they are connected to closed individuals. They're also more inclined to believe in strange things.

2.6.2 Theory of Interpersonal Behaviour (TIB)

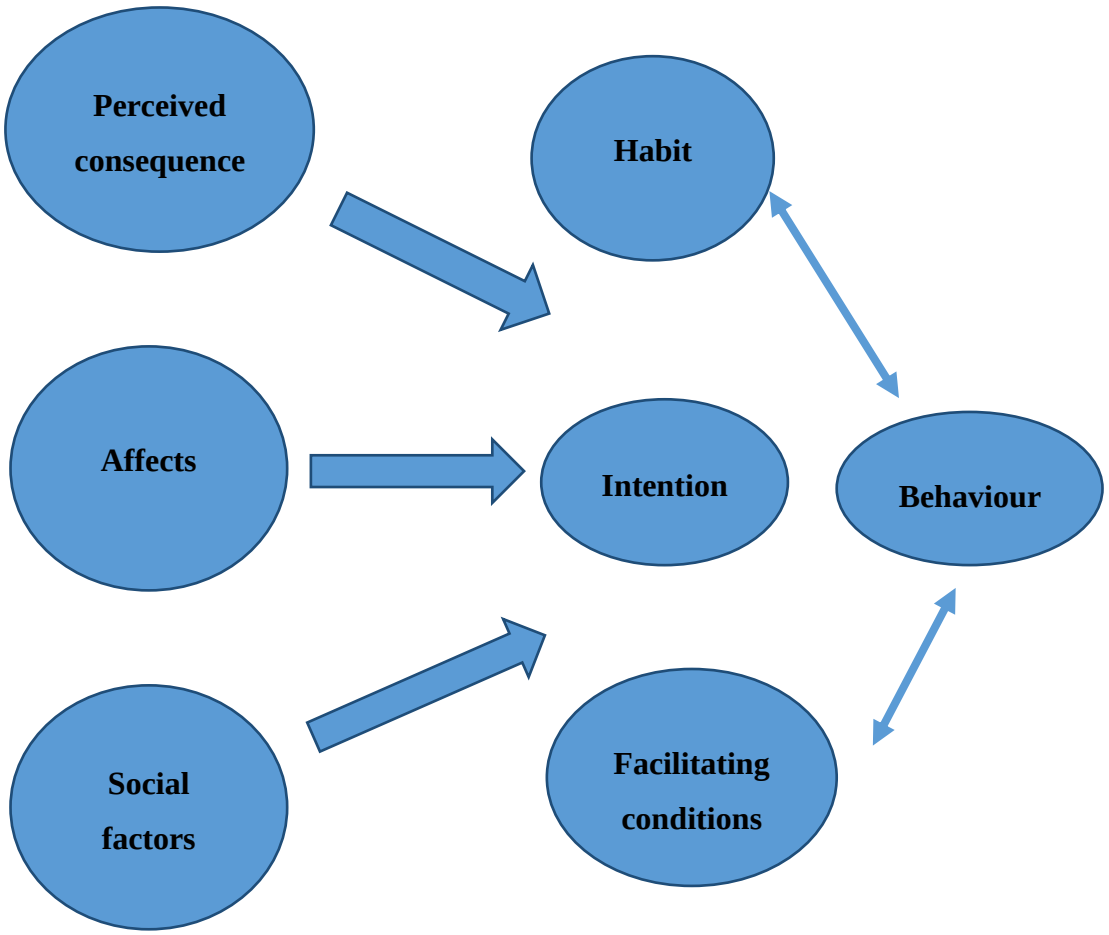
TIB is useful in determining the elements that influence cyber-loafing behaviour. Intention, habit and conducive conditions all play a role in adopting a specific behaviour (Chen *et al.* 2017: 36). Furthermore, TIB is extensively utilised to predict cyber-loafing activities. In this study, TIB was used to afford a better understanding of the individual actions that contribute to and lead to the participation in cyber-loafing activities. TIB is a model that considers three determinants of behaviour intention social factors such as facilitating conditions, habits and behavioural intentions (Khansa et al. 2017: 29).

Individuals' actions are the outcome of their behavioural intentions, according to the TIB, whereas behavioural intentions are direct functions of emotion, perceived consequences and social variables (Amin *et al*. (2016: 22; Issock and Mpinganjira 2020: 45). Furthermore, perceptions of the availability or lack thereof of necessary resources and opportunities; for example, including enabling resources) are antecedents of facilitating conditions (Kaptangil 2021: 21). It is for these reasons that TIB has been frequently adopted in other studies, as it is claimed that it best explains the cyber-loafing phenomenon. The extent to which an individual considers cyber-loafing behaviour to be good or negative as perceived outcomes is depicted in Figure 2.2.

TIB can assess the overall effects of accessing the Internet to do non-work and work-related tasks while utilising office resources. The sensation of being treated fairly at work by management or peers is referred to as the effect. Employees' feelings that push them toward online loafing include contentment, pleasure, despair, dislike and disapproval. A person who likes cyber-loafing is more likely

to utilise the Internet for cyber-loafing purposes (Hosseini, Reza and Farkhad 2015: 23). The level at which social groups interact is referred to as the social factor.

Figure 2. 2 Theory of Interpersonal Behaviour



Source: Chang and Cheung (2001)

Environmental variables that contribute to persons executing or completing their job tasks, resulting in specific behaviour, are referred to as facilitating circumstances. External conditions and resources, as well as internal conductions, are two types of facilitating conditions for self-efficiency (Sage 2015: 33). If an employee feels that their employers are monitoring their online resource consumption, he or she is less likely to indulge in cyber-loafing. As a result, an

employee who likes cyber-loafing may not be given an internet connection at work, preventing them from doing so.

2.7 GAP IN LITERATURE

Previous studies have focused on discovering different types of cyber-loafing activities among employees, breaking down cyber-loafing into two categories, minor cyber-loafing and serious cyber-loafing (Tandon, Kaur, Ruparel, Islam and Dhir 2021: 97; Dooly 2021: 56; Aku 2017: 45; Khansa 2017: 54). However, there is no evidence of studies that focused on an evaluation of tools used by the manager to control cyber-loafing by administrative staff. Evidence is needed to assist in the evaluation of the effectiveness of tools used to curb cyber-loafing activities by administrative staff. If the manager is successful in evaluating the cyber-loafing tools, it could assist the management to utilise more effective tools, identify strategies that no longer assist in decreasing cyber-loafing activities and if they need to suggest or discover a new tool that can be applied by managers in the future.

2.8 CONCLUSION

The opening of this chapter was to introduce the topic and defined the scope of this section. The starting point of this chapter was to introduce the topic and define the scope of this section. The other sub-topics of the chapter presented the definition of the key concepts used in this study, a literature study of cyber-loafing behaviours that occur among administrative personnel and a review of academic material that supports the manager’s use of cyber-loafing tools. In addition, the theories, including TIB and GDT as control tools supporting this study were presented. The chapter also identified and explained the factors that influenced or impacted the ability of the mitigating tools to be effective. The next chapter presents the methodology employed for this study.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The previous chapter presented a literature review of different studies related to this research and discussed the theoretical frameworks that were adopted in this study. This chapter presents the research methodology employed to achieve the objectives of this study. The research methodology forms an important part of any research study since the quality of the research outcomes is determined by the quality of data collection and the research methods employed. Hence, the main objective of this chapter is to explain the research design and methods used to underpin this study. In addition, this chapter describes the data collection method and the research instrument and the sampling method employed. Furthermore, this chapter presents how the researcher ensured the validity and reliability of the data collected, as well as how ethical principles were upheld.

3.2 RESEARCH DESIGN

Bhasin (2019: 14) points out that a research design is a step-by-step procedure that illustrates how a researcher conducts a scientific investigation. It includes so research methods that a research problem may be effectively managed (Kanholkar and Dharkar 2022: 45). Research design specifies the data collection strategy, the unit of analysis, the survey structure utilised for data gathering and the sort of outcomes the study is aiming for. To achieve the objectives of this study, a descriptive research design was employed. A descriptive design is useful when a study entails describing the characteristics of an already known phenomenon (Pandey and Pandey 2021: 45). In the context of this study, the descriptive research design was used to investigate and evaluate the tools used by the manager to prevent and control cyber-loafing in the workplace.

3.3 RESEARCH APPROACH

Nguyen (2019: 45) identified two types of research methods, namely quantitative and qualitative. A quantitative method is employed for a study that seeks to measure or quantify the research findings, while a qualitative method is employed when the study seeks to answer the questions of “how” and why” about a phenomenon being studied. Schoonenboom and Johnson (2017: 54) also noted that the qualitative method allows for an in-depth understanding of the phenomenon under investigation. In this study, the researcher employed a mixed method, which is a methodology that combines the elements of qualitative and quantitative research approaches. This is considered to gain an in-depth understanding of the phenomenon and to strengthen the validity of the findings (Dudovskiy 2016: 10). Combining both methods qualitative and quantitative enables the researcher to balance the limitations of each method and doing so provides strong evidence affording more confidence in the findings (Creswell 2017: 63).

3.4 TARGET POPULATION

A target population is a group of people with similar traits who are identified as the target audience for research (Monette, Sullivan and DeJong 2015: 5). This study's population consisted of managers, supervisors and administrative personnel of eThekwini Municipality Sizakala Customer Service. The eThekwini Municipality Sizakala Customer Service has 32 locations in KwaZulu-Natal. According to the centre’s human resources manager, the total number of workers who use computers to conduct their work obligations is around 423. This comprises permanent and contract administrative workers, managers and supervisors as shown in Table 3.1.

Table 3. 1 Population size

eThekwini Municipality Sizakala Customer Care	Total
Managers	5
Supervisors	6
Administrative Staff	382
Total	**393**

3.5 SAMPLING PROCEDURE

Sampling is the process of picking a subset of a population to participate in a study (Albers 2017: 44). As cited by Kanholkar and Dharkar (2022: 33), it is the process of selecting a group of people for research in such a manner that they represent the big group from which they were chosen. This study employed a purposive sampling approach, which is a non-probability sampling method in which elements for the sample are picked based on the researcher's judgement (Dudovskiy 2016: 44). The numerous strategies made feasible by the purposive approach afforded the research designs to be more flexible, allowing for particular techniques to be used when necessary to work toward the desired result. eThekwini Municipality Sizakala Customer Service has many divisions and positions according to the numbers that were presented by Bongi Madondo (Human Resources Manager, 2021). Each division and site are crucial for the business to be successful, hence using purposive sampling was best suitable for the researcher to fulfil the needs of the study. A few elements of the divisions were selected, namely, managers, supervisors and administrative personnel.

3.5 SAMPLE

The sample size, according to Nguyen (2019: 56), is the total group of units under consideration in a target population. Sample size plays a crucial role in the generalisability of research findings. A small sample size limits the study’s

findings to a subgroup in the target population. Nandi and Platt (2017: 56) noted that there is no specific rule for the selecting the sample size for qualitative study. Creswell (2017: 63) also indicated that the selection of the number of participants in the study should be based on the dimension (breadth, depth) the researcher intends to investigate. Considering that this study used mixed-method research, the sample sizes were categorised into quantitative and qualitative as discussed below.

3.5.1 Quantitative sample size

The sample size for the quantitative data was based on a 95% confidence level with an 80% proportion of the target population at 0.005 acceptable margins of error, using the following formula:

$N = \{Z^2 * \Sigma^2 * [N / (N - 1)] / \{ME^2 + [Z^2 * \Sigma^2 / (N - 1)]\}$. Whereby N= Sample Size; Z= Confidence Level; Σ = Alpha; P= Proportion and ME= Margin of error. The sample size for the administrative staff was 156.

3.5.2 Qualitative sample size

As determined by Nayak and Singh (2021 26), the rules for selecting the number of respondents to partake in a study depend on the research methodology. According to Patton (1990: 54), there are no specified rules for measuring the sample size in qualitative research. It is dependent on the dimensions (depth or breadth) in which the researcher seeks to inquire. Hence, the sample size for this study was 12 managers and supervisors, which conforms with Creswell (2017: 58), who indicated that 42 participants (managers and supervisors) suffice for a qualitative study.

3.6 DATA COLLECTION

A measuring tool is used to collect data on the sample chosen for the inquiry (Dudovskiy 2018: 05). Mixed methods data gathering is quite helpful in

deciphering discrepancies between qualitative and quantitative results, as well as qualitative discoveries.

3.6.1 Quantitative data collection method

To obtain quantitative data, questionnaires were used. As pointed out by Singh (2022: 44), questionnaires are a form of data collection that entails asking subjects to reply to a series of spoken and written questions. The advantages of employing this approach include being the most cost-effective option and a practical way and speedy way to collect data (Nguyen 2019: 56). On the other hand, it enables researchers to collect information from a huge number of individuals while also making data analysis simple (Nandi and Platt 2017: 02). Only administrative personnel were given the chance to respond to survey questionnaires in this study, questionnaires were handed out physically to 156 participants

3.6.2 Questionnaire Structure

The questionnaire used in this study contained 30 questions and it employed a five-point Likert scale. The questions were divided into 4 sections.

***Section A demographic**:*

This section contained questions that were aimed at obtaining the demographic information of the participants. The demographic information obtained includes the age, gender, ethnicity and qualification level of the participants.

Section B: Cyber- loafing activities

This section investigates cyber-loafing activities that are common among administrative staff. This section employs eleven questions.

Section C: Tools used to detect cyber- loafing activities

The section was aimed at investigating tools used by managers to control cyber-loafing activities

Section D: Factors affecting the implementation of tools

The section investigates factors affecting the implementation of tools that can be used to control cyber-loafing activities by administrative staff.

3.6.3 Qualitative data collection method

Interviews were conducted to acquire qualitative data. According to Singh (2022: 54), a qualitative interview is a discourse between a researcher and an interviewee to gather information. Interviews can be conducted over the phone or in person. This approach allows researchers to read nonverbal communication about the topic and the interviewer has control over the interviewee, allowing for more accurate screening of demographic questions. Interviews were conducted in person with managers and supervisors from eThekwini Municipality Sizakala Customer Care.

3.6.4 Interviews

As part of the data collection process, managers and supervisors were interviewed. The interviews used to gather qualitative data, on the other hand, are more organised, with researchers asking just a limited number of questions. Three sorts of interviews are used to obtain data. Telephonic interviews ruled the data collection methods charts for years. However, conducting video interviews through the Internet, Skype and other online video conferencing platforms are becoming increasingly common.

Face-to-face interviews are a tried-and-true way of collecting data directly from participants. It facilitates the collection of high-quality data by allowing for the use of extensive questions and extra probing to obtain rich and detailed information.

(Boterman 2021: 06). Regardless of the participant's literacy demands, face-to-face interviews offer plenty of opportunities to collect nonverbal data through observation or to delve into complex and unfamiliar topics. Despite being more expensive and time-consuming, face-to-face interviews provide greater response rates than internet interviews (Mohajan 2018: 64).

The researcher personally conducted the face-to-face interviews because screening can be done precisely. Face-to-face interviews help to ensure that candidates are properly screened (Nandi and Platt 2017: 02). The individual being questioned cannot provide incorrect information while answering screening questions such as gender, age, or race.

The interviewer is in command of the conversation and must be able to keep the interviewee interested and focused on the task. Face-to-face interviews are unquestionably effective for capturing the interviewee's emotions and behaviours. Schoonenboom and Johnson 2017: 55) advise keeping track of participants emotions and behaviours by observing them and writing them down. Face-to-face interviews are usually more costly on online interviews (Creswell 2017: 63). This study's interview questions were divided into three sections under the following headings:

A. Background Information: In this phase, research participants are asked questions about their age, gender, ethnicity and academic level.

B. Managerial tools for policing administrative staff's cyber-loafing activities: This question aims to analyse the study's respondent's tools and methods for minimising cyber-loafing activities among the administrative staff of eThekwini Municipality Sizakala Customer care, as well as unpacking those tactics for the researcher to evaluate the usefulness of such tools.

C. Factors influencing the use of measures to prevent administrative personnel from engaging in cyber-loafing: This part focuses on identifying the hurdles that respondents have when it comes to implementing methods to limit cyber-loafing

and it helped the researcher come up with suggestions and recommendations to address such issues.

3.7 DATA ANALYSIS

In this study, convergent parallel design data analysis was used. As believed by Creswell (2017: 66), the convergent design technique is the most common form of mixed-method research. The benefit of employing this technique is that data from both systems are collected at the same time, saving time (Mohajan 2018: 33).

3.7.1 Quantitative data analysis

The researcher used Statistical Package for the Social Sciences (SPSS, Version 27) to analyse the quantitative data. The researcher used frequencies, cross-tabulation and bivariate statistics to analyse data for the quantitative research strategy (Polit and Beck 2012: 63). Statistical measures, analyses and trustworthy data interpretation, the researcher employed concurred with the statistical analysis.

3.7.2 Qualitative data analysis

The researcher used the narrative technique to analyse data acquired through interviews for the qualitative research methodology. Mitchell and Egudo (2013: 6) describe a narrative method as a social science strategy that incorporates the use of storytelling methodology to assist the researcher gain insight into organisational information and aid in the transmission of diverse tacit information. The storytelling approach can also be used to establish implicit communication (Ramalingam and Jiar 2022: 58). A narrative technique (also known as a literary fictitious, literary technique, literary device, or fictional device) is a method of conveying information to the audience and enhancing the story's completeness, sophistication, or interest (Nayak and Singh 2021: 55).

3.7.3 Thematic analysis

A thematic analysis method was used by the researcher to transcribe interviews. Thematic analysis is a qualitative data analysis technique that entails reading through a data collection (such as transcripts from in-depth interviews or focus groups) and looking for trends in meaning across the data to deduce themes (Byrne 2022: 65). Thematic analysis is an active process of reflexivity in which the researcher's subjective experience is essential to deriving meaning from evidence (Thomson 2022: 45)

Byrne (2022: 65) postulate that the thematic analysis is a versatile method to qualitative analysis that allows researchers to draw new insights and concepts from data. One of the many advantages of theme analysis is that novice scholars who are just learning how to evaluate qualitative data will find it an accessible method.

3.8 RELIABILITY AND VALIDITY

The reliability testing of this study was done using Cronbach's alpha. The main purpose was to test the consistency and reliability of the research questions. According to Taherdoost (2016: 66), the Cronbach alpha coefficient is the most appropriate measure of reliability when measuring the reliability of a Likert scale. It is further reiterated that the results of the reliability testing should have a minimum internal consistency coefficient of 0.70. The results of this study show that the internal consistency was 0.782, which is a good measure.

To ensure the study's credibility, the researcher endeavoured to eradicate any bias and generate convincing findings. Triangulation of the data was utilised to check for similarity and diversity of various replies to assess internal consistency and efficient dependability to the investigation. This strategy, according to Dudovskiy (2018: 5), is the rewriting of stories told through interviews.

The study's validity was guaranteed by conducting a pre-test. Before the final questionnaires were handed to the participants, the questionnaire was subjected to pretesting to identify errors that may be encountered by the participants (Mohajan 2018: 66). In addition, the pretesting was considered imperative to uncover any lack of clarity, ambiguity, or bias, that may be present in the questionnaire (Bhattacherjee 2012: 36).

The questionnaire was presented to a group of seven administrative staff members and two interviews were conducted: one with a manager and one with a supervisor who was part of the target demographic. The researcher requested that the participants express their worries about the questionnaire and interview while filling out the questionnaire and during the pretesting of the interviews.

All of the concerns highlighted were considered and addressed throughout the preparation of the final questionnaire and the questions designated for managers were amended accordingly. Concerns were raised about the tiny font size, the usage of foreign terms and the similarity of questions. The total number of nine participants who took part in the pretesting were excused from the study's sample. Furthermore, the data gathered during the pretesting was isolated from the data collected during the final questionnaire and interviews and it was likewise exempted from data analysis.

3.9 DATA QUALITY

It is essential consider data quality in any study. In quantitative research, internal and external validity, reliability and objectivity are criteria for data quality, while in qualitative research, trustworthiness criteria, which include credibility, transferability, confirmability and dependability are used to ensure data quality (Lincoln *et al.* 1985: 66). As mentioned by Erlandson (1993: 132), "trustworthiness is established in a naturalistic inquiry by the use of techniques that provide true value through transferability, consistency through dependability and neutrality through confirmability". To demonstrate data quality, avoid bias and

increase the trustworthiness of the data collected in this study, the following were considered (Grover 2015: 45):

3.9.1 Transferability

Transferability is a way of achieving generalisation in qualitative research. Although generalisation is said to be limited in qualitative studies, the research methods and context need to be explicit enough for the reader to determine the adaptability of the study in their own context. Krzych, Lach, Joniec, Cisowski and Bochenek (2018: 45) recommended thick description and purposive sampling as ways of increasing the transferability of qualitative research.

A thick description aids transferability as it requires an explicit definition of the research methods, perspectives and context of the study. The purposive sampling adopted for this study increases transferability by allowing the researcher to select only specific experts who have experience with the research phenomenon or questions. In this study, thick description and purposive sampling were used to increase the transferability of the study.

3.9.2 Credibility

Credibility is the degree of confidence that the findings of a study are true and accurate. According to Lincoln *et al*. (1985: 96), the methods that could be used to increase the credibility of a study are persistent observation, prolonged engagement, member checking and triangulation. Persistent observation requires that the researcher identify the characteristics that are most relevant to the objective of the study and focus on them. Prolonged engagement demands that the researcher spends sufficient time engaging the respondents to increase the rapport and trust between both parties. Member checking is the participants' validation of a researcher's inferences.

Triangulation is the simultaneous use of different types of research elements, such as data sources, methods, or theories, in verifying and proving the accuracy

of the findings of the study. In this study, member checking was used to increase the credibility of the research findings. According to Taherdoost (2016: 86), it is a method used by researchers to increase the trustworthiness of the results of a study by returning the analysed data or findings to respondents to check for validity. Member checking was applied in this study by sending the analysis of the interviews back to the participants to give feedback on areas of agreement and divergence.

3.9.3 Confirmability

Confirmability is the extent to which the findings of the study are neutral and not influenced by the researcher's bias, interest, or motivation (Creswell 2017: 66). As reported by Dudovskiy (2018: 69), confirmability can be assured by providing an audit trail, which is the archiving of all materials and instruments used during the investigation. To ensure the confirmability of this study, the following have been securely archived for record and recall purposes for five years:

a) ***Raw data*** – all raw data, field jotters and interview records.

b) ***Data reconstruction products*** – notes from coding the interview transcripts, findings and conclusions and a final report including connections to existing literature and integration of concepts, relationships and interpretations.

c) ***Process notes*** – all jottings relating to the methodology (procedures, design plan and rationale), trustworthiness notes (about credibility, dependability and confirmability) and audit trail notes.

d) ***Materials about study purpose and dispositions*** – including the researcher's jottings on personal thoughts, expectations and motivation.

e) ***Instrument development information*** – pilot interview schedule and versions of the revised interview schedule.

3.9.4 Dependability

Dependability is the extent to which the study is consistent and repeatable. One of the major ways of improving the dependability of a study is through an external audit (Nandi and Platt 2017: 56). An external audit involves having an independent researcher review the methods and activities used in achieving the objective of the study. To assure the dependability of this study, an independent researcher (selected based on experience and expertise in qualitative research) examined the research process, which included the analysis of the interviews, findings and conclusions (Albers 2017: 45). The examination was to evaluate the accuracy and coherence of the interviews, findings and conclusion.

3.10 ETHICAL CONSIDERATION

As one of the requirements of scientific research, the study followed all the scientific principles as well as the university's ethical principles. In this regard, ethical approval for this research was obtained from the DUT ethics committee. Furthermore, to guarantee that integrity was upheld, the researcher handed out informed consent forms to the respondents, which permitted the respondents to decide whether or not to partake in the study. Confidentiality was maintained by ensuring that the participant's responses and personally identifiable information were not disclosed to any third party.

3.11 CONCLUSION

This chapter presented the research methodology, sampling and data collection techniques that were used to achieve the objectives and obtain the findings in this study. A mixed-method approach was implemented and data was obtained through questionnaires and interviews. Interviews were conducted with managers, supervisors, and administrative staff (questionnaires). A purposive sampling technique was used to select the sample required for the study. Analysing the quantitative data was done using SPSS Version 27 (Statistical

Package for the Social Sciences). Interviews were transcribed using a thematic analysis method by the researcher. The research was carried out at eThekwini Municipality Customer Service in Natal.

The next chapter presents the result of the data analysis.

CHAPTER FOUR

DATA PRESENTATION

4.1 INTRODUCTION

This chapter presents the study findings gathered from various administrative workers, managers and supervisors of eThekwini Municipality Sizakala Customer Care . The findings were collected using a closed-ended questionnaire targeted at administrative staff and an open-ended interview questionnaire targeted at managers and supervisors. The findings are presented in graphs, tables and pie charts. As part of the analysis, this chapter begins by analysing the participants' biographical information, which includes their gender, age and qualifications. The purpose of structured data collection was to determine the following:

- To identify cyber-loafing activities common among administrative staff at eThekwini Municipality Sizakala Customer Care.
- To determine the tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer Care.
- To examine factors affecting the implementation of tools that can be used by management to control cyber-loafing by administrative staff in eThekwini Municipality Sizakala Customer Care.

In chapter three, the methods of data gathering and analysis were covered. The research findings are described in this chapter. The findings were used to discover recommendations for tools and strategies to mitigate cyber-loafing in the workplace using the case study of eThekwini Municipality Customer Care.

4.2 RESPONSE RATE

This section presents the quantitative and qualitative response rates.

4.2.1 Quantitative response rate

For the quantitative research, 101 participants were able to respond to the questionnaires, giving a response rate of 65%. According to Taherdoost (2016: 69), the normal or appropriate sample size for quantitative research studies is 40% of the participants.

4.2.2 Qualitative response rate

A total of 11 participants participated in the data collection process by way of interviews, giving a response rate of 92%. As per qualitative studies, it has been recommended that qualitative research studies require a minimum of 10 participants (Kumar 2014: 56). This means that the findings of this study are based on an acceptable response rate.

4.3 QUANTITATIVE DATA ANALYSIS

This section presents the quantitative data analysis gathered through the questionnaire.

4.3.1 Biographical information

The biographical information of participants who participated in the study is presented in this section. Participants were requested to present their age, gender and academic level.

4.3.1.1 Age of participants

Figure 4.1 shows the age group distribution of participants. It shows that most participants (41.6%) fall in the age group of 31-40 years, whilst 34.67% fall in the age group between 18 and 30 years. The findings also show that 14.9% are between 41 and 50 years and 8.8% being the minority, are 51 years and above. Based on the findings, young people considered being youths between 18 and 34 dominate the organisation. In the study by Huri and Sacip (2015: 39), it was

commented that younger people are more likely to engage in cyber-loafing and using the Internet for personal reasons than the older generations. Older people normally comply with the organisational policies when using the Internet, while young people violate the norms. However, even though academics have provided more factual evidence for the age gap, more study is still needed to draw conclusions.

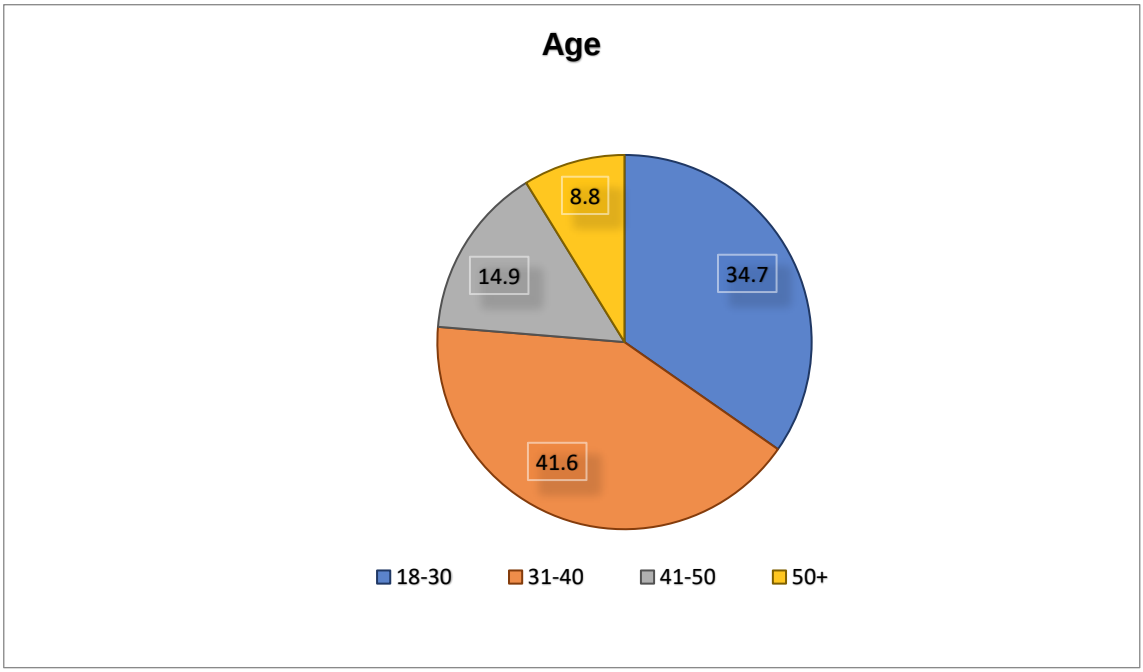


Figure 4. 1 Age of participants

4.3.1.2 Gender of participants

The study assessed the gender distribution of participants, as shown in Figure 4.2. It is evident that the majority (52.5%) of the participants were female, whilst the minority (47.5%) were male. From the above findings, it can be argued that female employees dominate the administration department of eThekwini Municipality Sizakala Customer Care. Gender has been regarded as an essential component in studying internet use habits such as cyber-loafing. Men are more likely than women to engage in cyber-loafing and are more likely to use the Internet while at work for personal reasons, which increases their risk of Internet

misuse (Kasap 2019: 103). However, research is required to evaluate potential errors in measuring methodologies and the operationalisation of independent variables.

When it comes to online shopping, men outnumbered women in a recent survey of Malaysia's millennial workforce (Dileep, Govindarajo, Normala and Othman 2014: 64). Although past research suggests that there is a gender difference in employee cyber-loafing and given the paucity of studies specifically on South African cyber-loafing, it is still necessary to explore this behaviour about gender among South African workers.

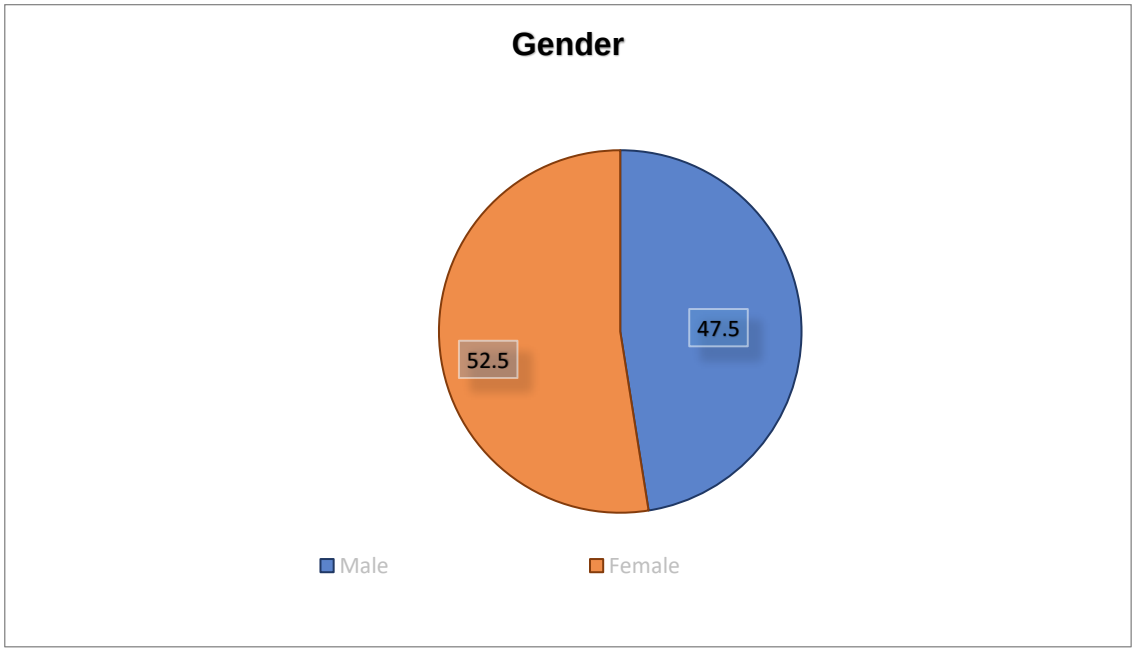


Figure 4. 2 Gender of participants

4.3.1.3 Academic Level of participants

The academic level of participants was also evaluated to determine their academic qualifications. According to Figure 4.3, 35.6% of those evaluated had matriculated. Degree holders made up 27.8% of the total, while those with certificates made up 18.8%, diploma holders made up 11.9% and the remaining 5.9% had only passed grade 11. This finding indicates that people in grade 11

are unfamiliar with computers; due to their lack of familiarity with computer programmes, they are unlikely to engage in cyber-loafing. On the other hand, individuals with matric find themselves under pressure to grow as a result of the pressure from their colleagues who have qualifications, so they find themselves using their employees' time to do their courses. Individuals suffer as a result of the pressure to obtain a qualification.

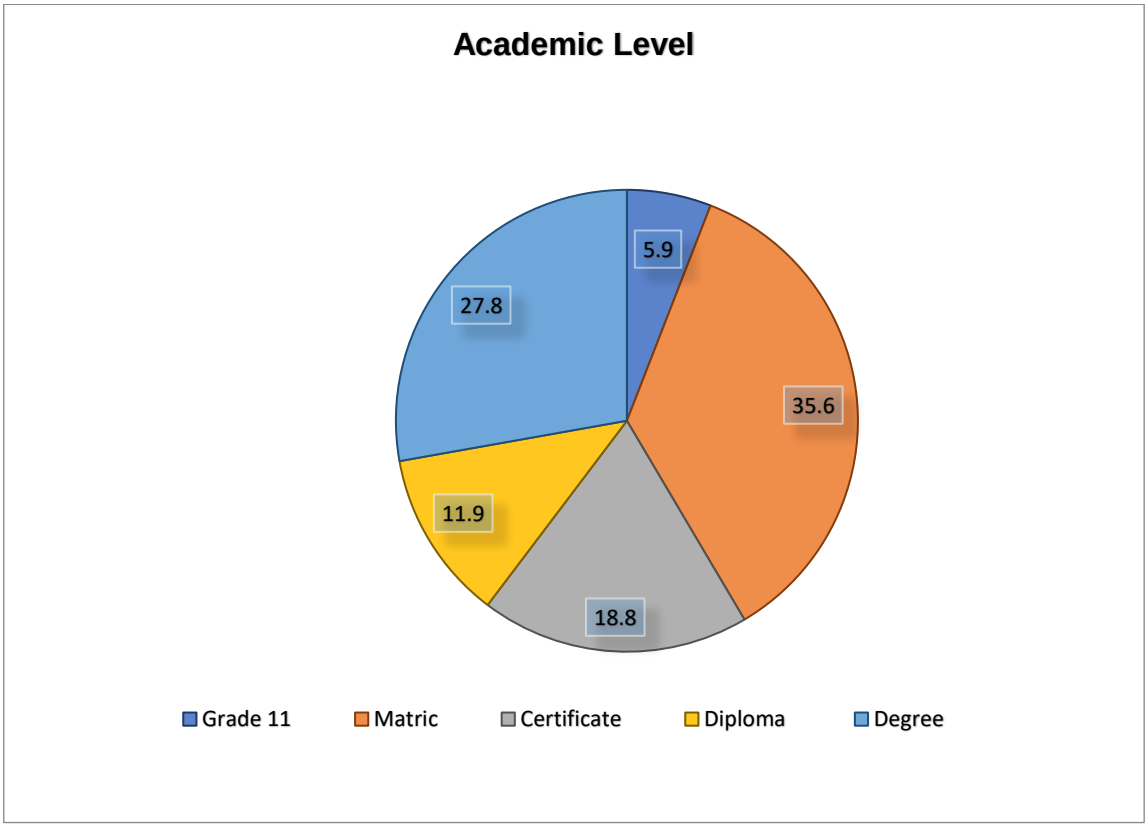


Figure 4. 3 Academic Level of participants

4.4 ANALYSIS OF RESULTS AS PER RESEARCH OBJECTIVES

The following section presents findings based on the research objectives from sections 4.4.1 to 4.4.3. As mentioned in the previous chapter, a Likert scale questionnaire was used to collect data and the following choices were available for participants (never, rarely, sometimes, often and always).

4.4.1 Objective 1: To identify cyber-loafing activities that are common among administrative staff at eThekwini Municipality Sizakala Customer Care

This part presents various cyber-loafing activities common amongst administrative staff at eThekwini Municipality Sizakala Customer Care . Participants were asked 11 questions. From the questions, the following activities were identified.

Online shopping, gaming and sports, visiting holiday and travel sites, visiting social media sites, accessing job search sites, pursuing studies, accessing online news, accessing online magazines, accessing auction sites, checking weather forecasts and accessing personal e-mails.

4.4.1.1 Online shopping

Figure 4.4 shows one of the cyber-loafing activities recorded in the study. Participants point out that they use their allocated work computers and the Internet to shop online. 17.8% said they have “never” engaged in online shopping, whilst 23.8% said they “rarely” do. On the other hand, 31.7% “sometimes”, 20.8% “often” and 5.9% “always” do online shopping. However, this confirms that online shopping is a cyber-loafing activity practised by administrative staff at eThekwini Municipality Sizakala Customer Care . This finding corroborates the finding by Aku (2017: 69), who also mentioned that online shopping is another type of cyber-loafing involving interactive internet activity.

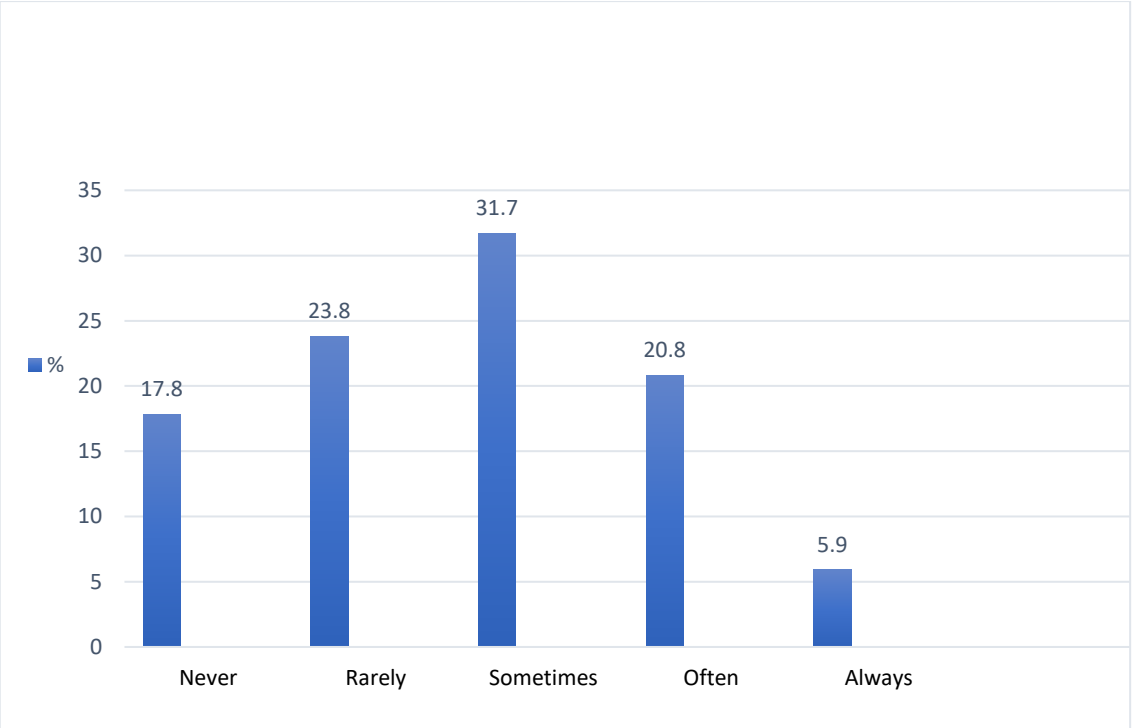


Figure 4. 4 Online shopping

4.4.1.2 Gaming and sports

Figure 4.5 presents the findings from the participants on whether they used their work computers and the Internet for gaming or sporting activities. 29.7% indicated that they “never” used their work computers and the Internet for gaming and sport whilst 16.8% indicated that they rarely participated in these activities. On the other hand, 16.8% indicated that they “sometimes” participated in these activities and 24.8% stated that they “often” participated and 11.9% mentioned that they “always” participated in this cyber-loafing activity. With the majority of the participants confirming that they engaged in this type of cyber-loafing activity, gaming and sports are, therefore, part of the cyber-loafing activities being practised in the workplace. To confirm the above finding, Kasap (2019: 89) reiterated that many employees engage in cyber-loafing activities to perform their duties, such as gaming and sports.

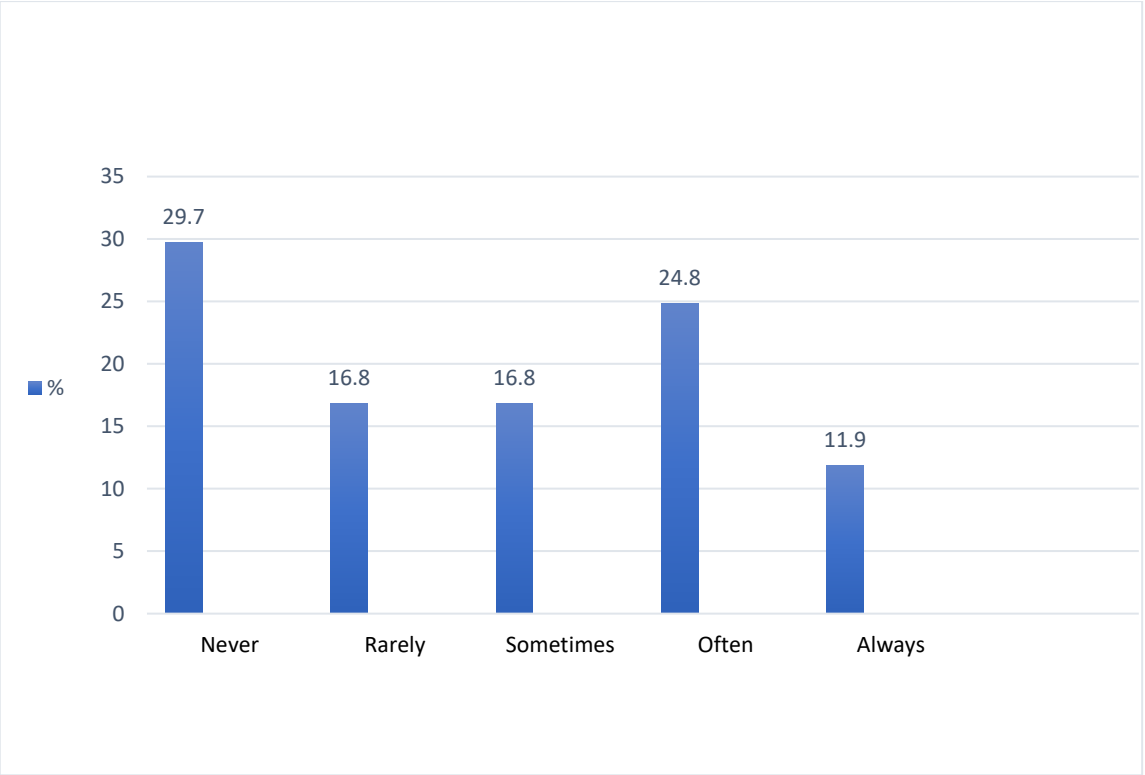


Figure 4. 5 Gaming and sports

4.4.1.3 Visiting holiday and travel sites

Figure 4.5 presents findings from participants on whether they used company computers and the Internet to visit holiday and travel sites. 13.9% indicated that they never used company computers and the Internet to visit holiday and travel sites, whilst 14.9% indicated that they "rarely" engage in such activities. On the other note, 31.7% indicated that they "sometimes" partake in these activities, 32.7% said they "often" engage in cyber-loafing and 6.8% indicated that they "always" use company computers and the Internet to visit holiday and travel sites. The majority of the participants confirmed that they engaged in this type of cyber-loafing activity. This confirms that visitation of holiday and travel sites is one of the cyber-loafing activities practised by administrative staff at eThekwini Municipality Sizakala Customer Care. The findings thus concurs with Karabiyik (2021: 89) that visiting holiday and travel sites was a common cyber-loafing activity among students in a class.

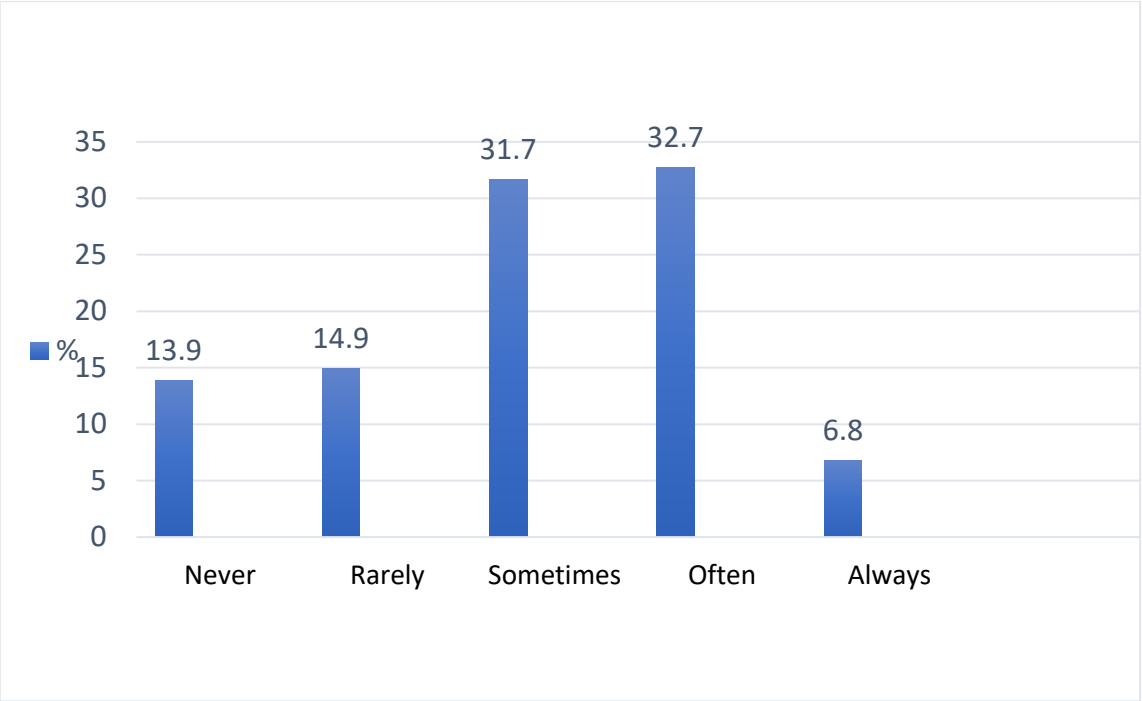


Figure 4. 6 Visiting holiday and travel sites

4.4.1.4 Social media sites

Another question posed to participants was whether they used company computers and the Internet to visit social media sites. Figure 4.7 below revealed that 8.9% and 9.9% rarely visited social media sites using company resources. On the other hand, 14.9% “sometimes”, 31.7% “often” and 34.6% “always” visited social media sites using company computers and the Internet. This confirms social media visitation as the leading cyber-loafing activity practised by administrative staff at eThekwini Municipality Sizakala Customer Care. According to Elciyar and Simsek (2021: 105), accessing social media platforms during working hours is an extreme or severe cyber-loafing activity.

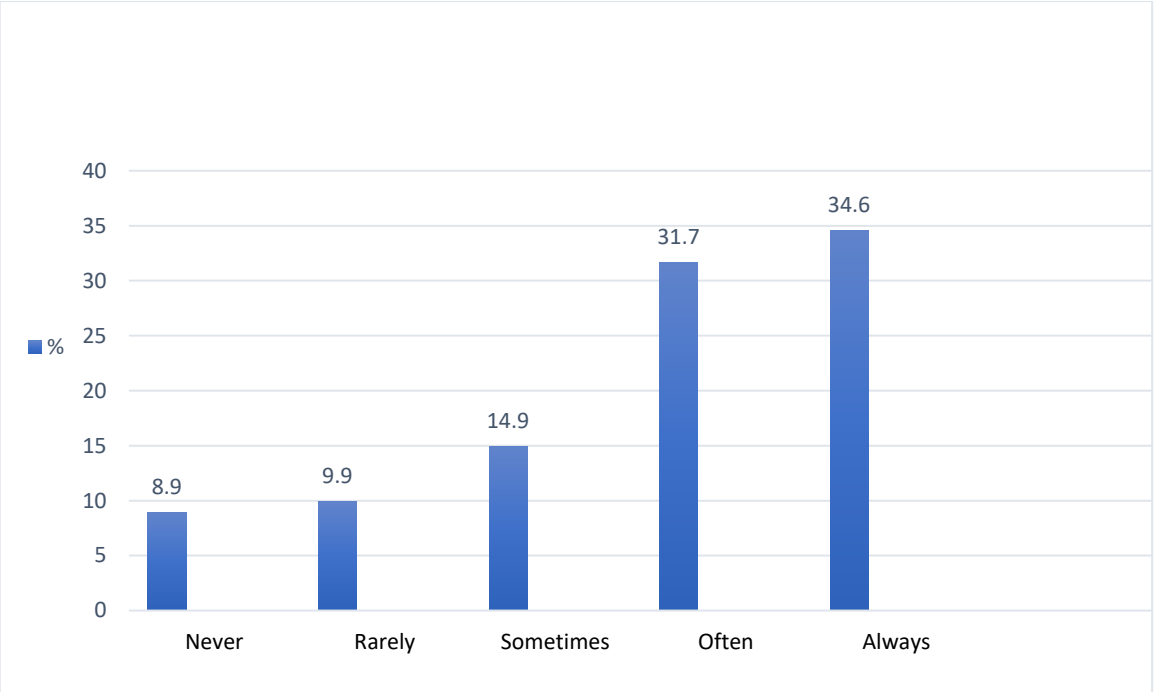


Figure 4. 7 Social media sites

4.4.1.5 Accessing job search sites

Furthermore, the study asked participants whether they used company computers and the Internet to search for jobs online. Figure 4.8 displays that 5% said they have never and 4% “rarely” use company resources to do job searches online. However, 19.8% sometimes, 40.6% “often” and 30.6% always use company computers and the internet search for jobs online. This confirms job searching is another popular and widely practised cyber-loafing activity among administrative staff at eThekwini Municipality Sizakala Customer Care . Şimşek and Şimşek (2019: 66) also confirmed that accessing recruitment platforms or searching for jobs on the Internet using company computers is another common form of cyber-loafing activity among employees in almost every organisation.

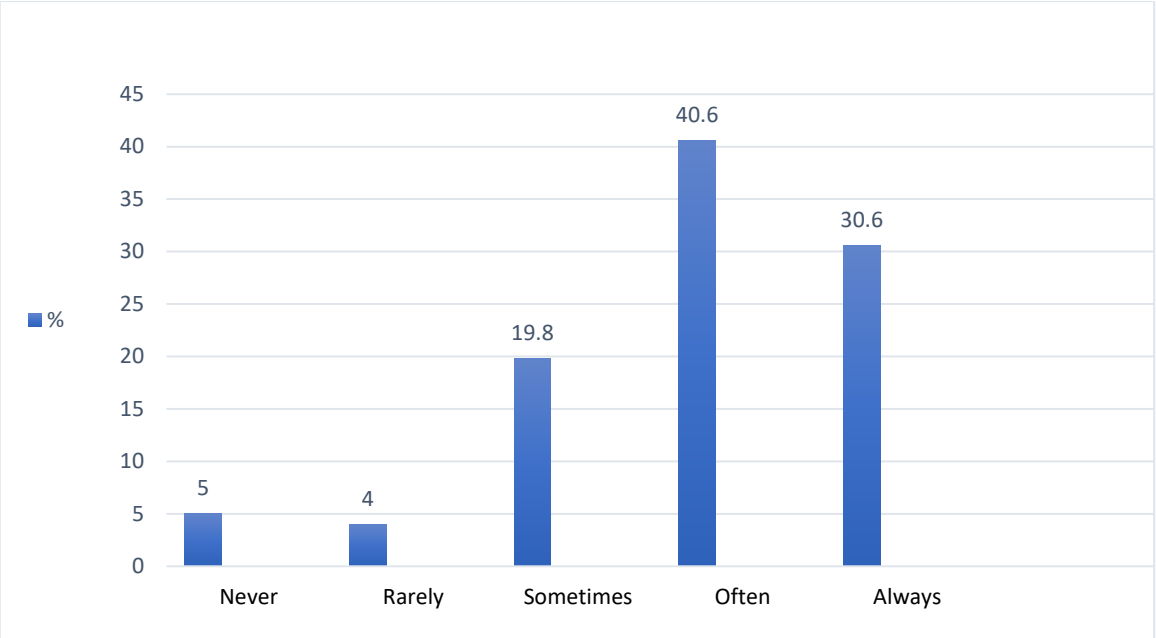


Figure 4. 8 Accessing job search sites

4.4.1.6 Pursuit of studies

Figure 4.9 presents the findings relating to a question posed to participants on whether they used company computers and the Internet to pursue their studies. 16.8% of participants indicated that they have never pursued studies using company resources, whilst 5% said they “rarely” participated in such activities. On another note, 16.8% said they “sometimes” partake in such activities. 28.7% also indicated that they “often” engage in such activities, whilst 32.7% said they “always” use company computers and the Internet to pursue their studies. The combined results for participants who rarely and always used the company resources indicate that there is a trend in internet usage. This could be attributed to the fact that participants are computer literate and want to pursue their studies to find better opportunities as they advance academically. Şimşek and Şimşek (2019: 54) echoed the same sentiment that online learning is a form of cyber-loafing activity that takes place over the Internet, which is officially known as e-learning, where employees can use their employer's Internet to pursue their studies.

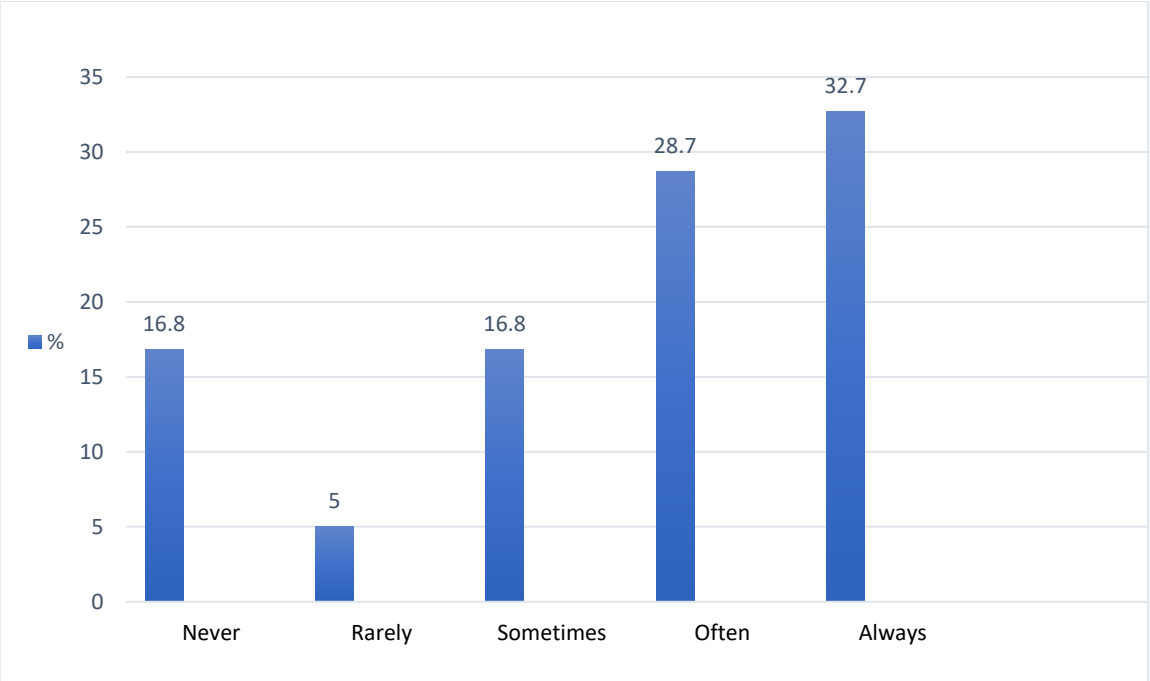
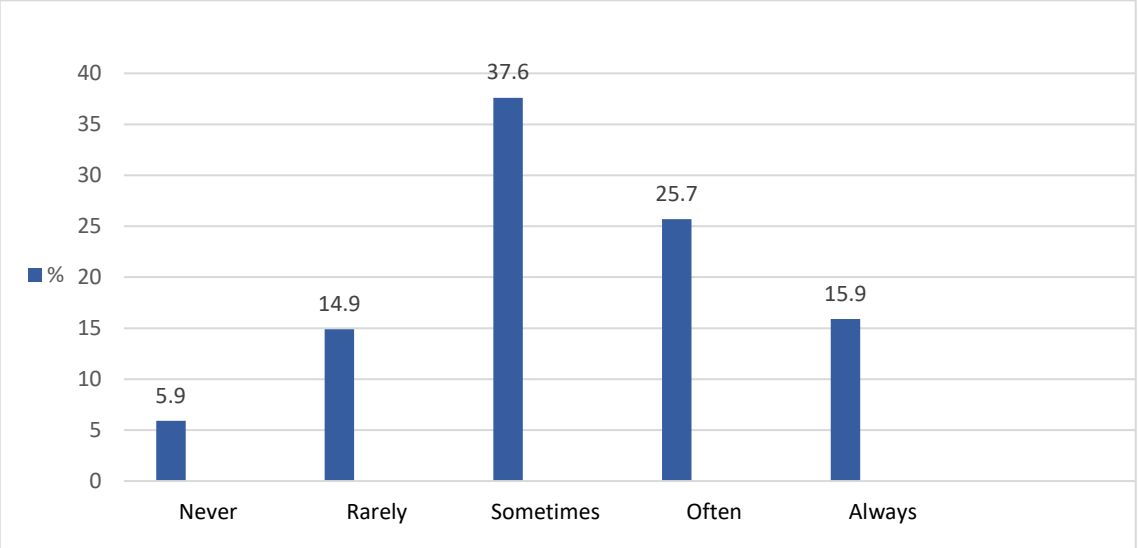


Figure 4. 9 Pursuit of studies

4.4.1.7 Accessing online news sites

The study also surveyed participants about whether they used company computers and the Internet to access online news sites. Based on the findings in Figure 4.10, it was revealed that 5.9% have “never” accessed online news sites using company resources, whilst 14.9% highlighted that they rarely engaged in such activities. The findings also indicated that 37.6% said they are “sometimes” involved in cyber-loafing. On the other end, 25.7% said they “often” engaged in such activities. Lastly, 15.9% of participants said they “always” visited online news sites using company computers and the Internet. With the responses that indicated “sometimes”, “often” and “always”, it can be deduced that accessing online news sites is another popular cyber-loafing activity being practised by administrative staff at eThekwini Municipality Sizakala Customer Care . In confirmation of the above findings, Jandaghi *et al.* (2015: 74) reiterated that cyber-loafing activities done by employees include reading the news on the Internet with company computers during working hours.

Figure 4. 10 Accessing online news sites



4.4.1.8 Accessing online magazines

Accessing online magazines is depicted in Figure 4.10. Participants were asked whether they used computers and the Internet to access online magazines. Findings reveal that 24.8% never used computers and the Internet to access online magazines, whilst 27.6% said that they “rarely” engaged in such activities. On the other hand, 34.7% said they access online magazines using their company computers. It is assumed that 34.7% of eThekwini Sizakala Customer Care staff have enough time to navigate the Internet and read an online magazine during working hours. A percentage of the participants, reflecting 12.9%, pointed out that they “often” used company resources to access online magazines. Therefore, the findings revealed that accessing online magazines was another cyber-loafing activity but was the least done activity. To confirm the above findings, Lim and Tee (2021: 68) found that university students, whilst in lectures, spent most of their time reading blogs, novels, comics and magazines online.

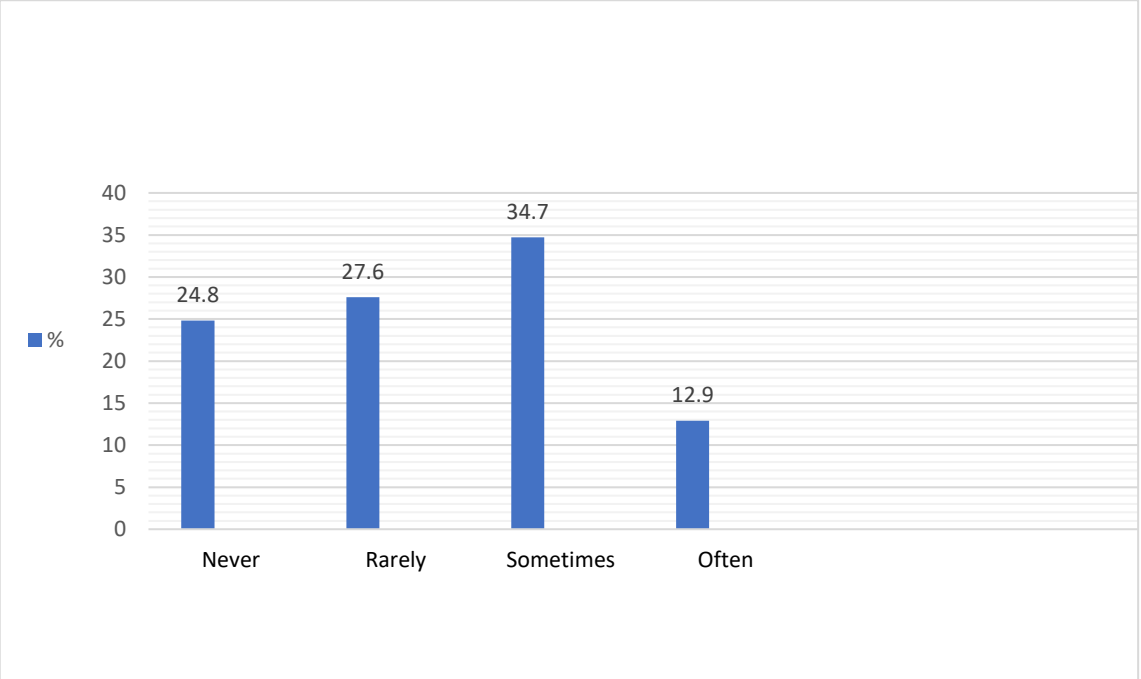


Figure 4. 11 Accessing online magazines

4.4.1.9 Accessing auction sites

As shown in Figure 4.12, another question was posed to participants on whether administrative staff used company computers to access auction sites. The findings revealed that 13.9% have never engaged in such activities and 15.8% said they rarely visited auction sites using company resources. However, 33.7% said they are “sometimes” involved in such activities while 28.7% confirmed that they “often” engaged in such acts. Only 7.9% said they used the company computers and internet to access auction sites. From the findings, it can be concluded that participants who “sometimes” and “often”, accessed internet sites to browse auction sites are indeed involved in cyber-loafing activities at the workplace. The findings further align with Toker and Saturday's (2021: 105)

findings that those students in a computer laboratory setting frequently participated in online auctions.

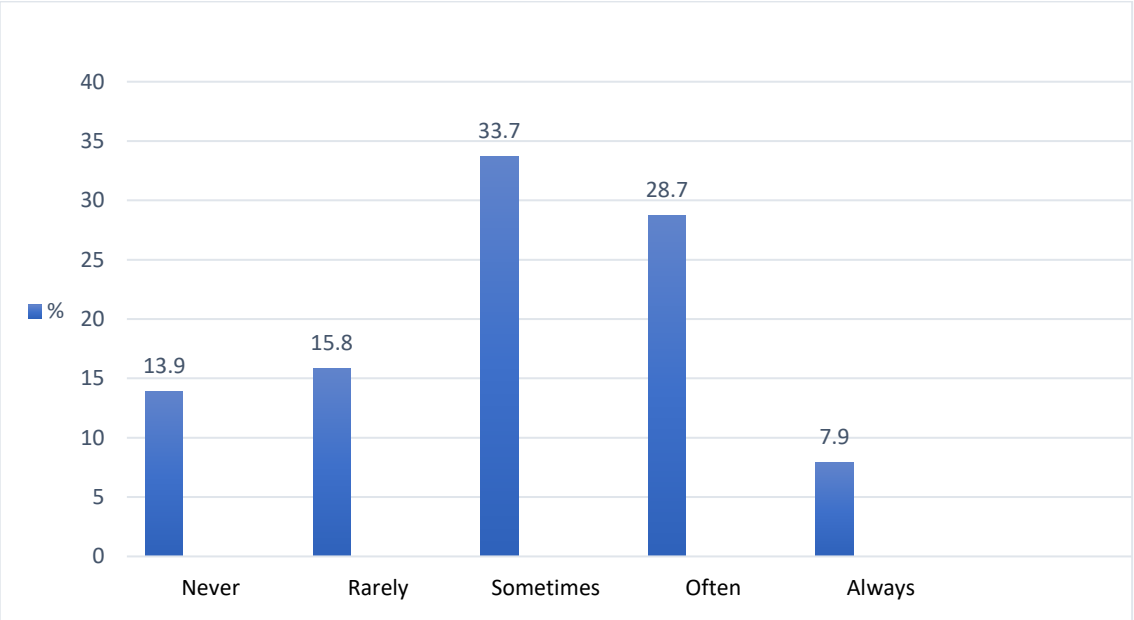


Figure 4. 12 Accessing auction sites

4.4.1.10 Checking weather forecasts

The findings under Figure 4.13 present the participants' responses on whether they use company computers and the Internet to access weather forecast sites. The study revealed that 4% have never used company computers and the Internet to access weather forecast sites, whilst 16.8% indicated that they rarely participate in these activities. On the other hand, 23.8% indicated that they "participate" in these activities, 24.8% stated that they "often participate" and 30.6% mentioned that they "always participate" in this cyber-loafing activity. The finding that 30.6% of participants have "always participated" in checking the forecasts indicates that staff at the eThekwini Municipality Sizakala Customer Care prefer to wear comfortable clothes as they check the weather. With the majority of the participants confirming that they engaged in this type of cyber-

loafing activity, checking the weather forecast is one of the most common cyber-loafing activities practised by administrative staff at eThekwini Municipality Sizakala Customer Care. The above findings are supported by Karabiyik (2021: 97), where an assertion is made that visiting weather forecasts is most common among some people in organisations as everyone is conscious about the environment.

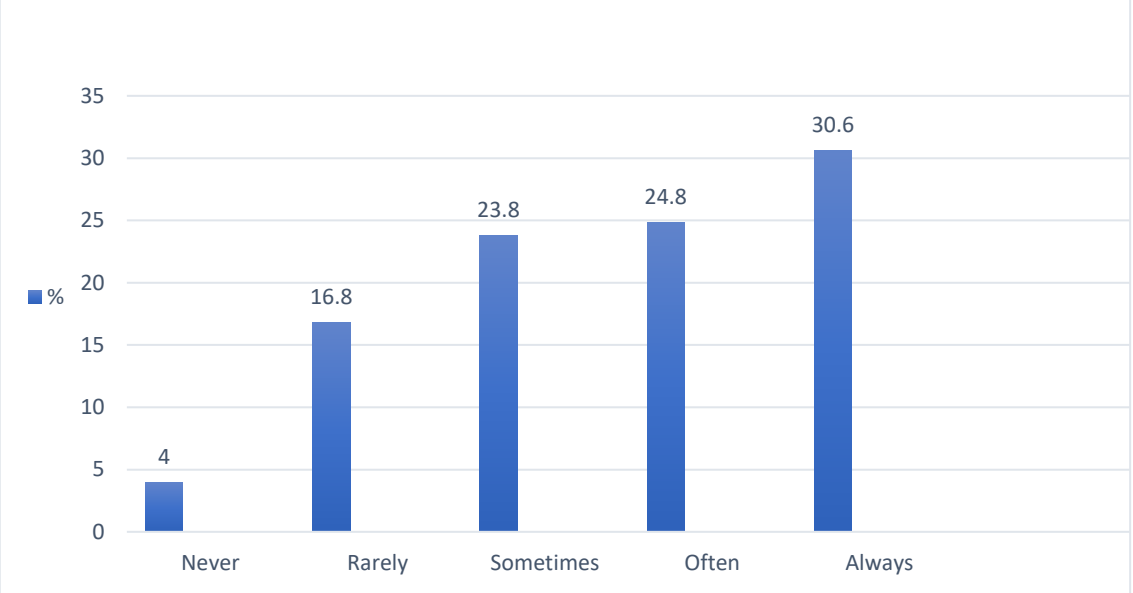


Figure 4. 13 Checking weather forecasts

4.4.1.11 Accessing personal e-mails

Accessing personal e-mails was one of the questions directed toward participants in cyber-loafing activities. From the findings in Figure 4.14, only 4% indicated that they have “never” used their work computers and the Internet to access personal e-mails using company resources, whilst 18.8% indicated that they “sometimes” partake in these activities. Contrary to the above findings, 20.8% pointed out that they often participate in accessing personal e-mails. In comparison, 56.4% confirmed that they always use computers and the Internet to access personal e-mails. From the responses of “often” and “always”, it is evident that a larger portion of participants was involved in accessing personal e-mails during working

hours using company resources. To confirm the above findings, Aku (2017: 69) reiterated that e-mailing is another type of cyber-loafing activity that involves receiving and sending e-mails for personal purposes using a company computer and the Internet.

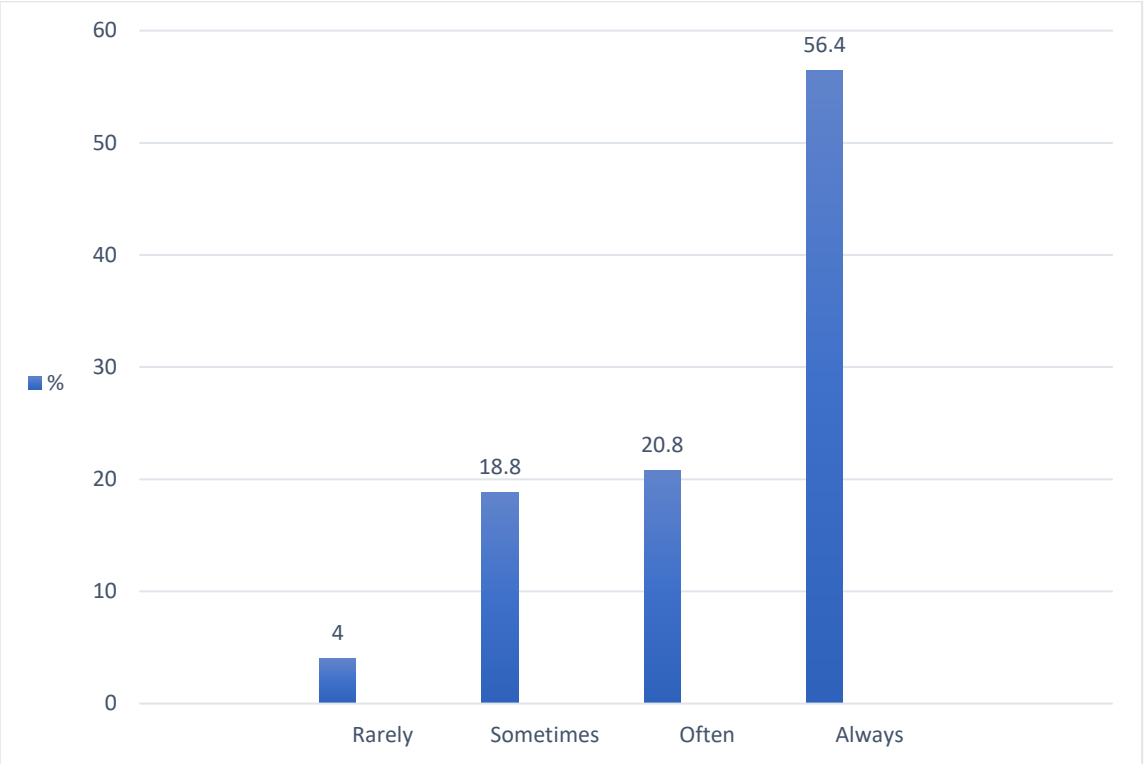


Figure 4. 14 Accessing personal e-mails

4.4.1.12 Conclusion of Objective 1

In summary and concluding the findings on objective 1, Figure 4.15 shows the type of cyber-loafing activities common among administrative staff at eThekwini Municipality Sizakala Customer Care, which have already been presented and discussed. The activities are ranked from the most used to the least used. The most prevalent cyber-loafing activities were found to be “accessing job search sites” and “personal e-mails”. It can be assumed that staff at eThekwini Sizakala Customer Care are job hunting and checking their e-mails to see if there are any job offerings or notifications that have come through. Figure 4.15 shows that

cyber-loafing was represented in varying percentages depending on the loafing activity.

Accessing personal e-mails was rated the highest among other activities at 96.04%. It can then be concluded that eThekwini Sizakala Customer Care staff were busy with personal e-mails instead of performing daily duties. The second was accessing sites for job searches at 91.08%. The combined results for, accessing personal e-mails and job searches further suggest that staff are accessing e-mails to establish if there are any job offers in their e-mail inbox. Accessing social media sites was rated at 81.18%. This finding suggests that staff were busy on social media, possibly interacting with their friends and family during working hours, which may hinder productivity.

Accessing weather forecast sites and online news was rated at 79.2%, being the fourth rated activity, according to figure 4.15. The pursuit of studies was also rated high at 78.21%. This finding could be attributed to the fact that staff at eThekwini Municipality Customer Care are pursuing their studies for better opportunities, either within or outside the eThekwini Municipality. Visiting holiday and travel and auction sites were ranked between 70% and 71%. This finding suggests that the activity is active within the organisation but less prevalent than accessing job sites and personal e-mails.

Accessing online shopping, gaming and sport, as well as accessing online magazines, were less popular. From the above findings, it may be assumed that staff at the eThekwini Sizakala Customer Care are not satisfied with their jobs and are demotivated since they are using company resources (internet and computer) to search for more jobs or checking on their e-mails. Checking personal e-mails is also linked to doing personal business while at work and using company resources.

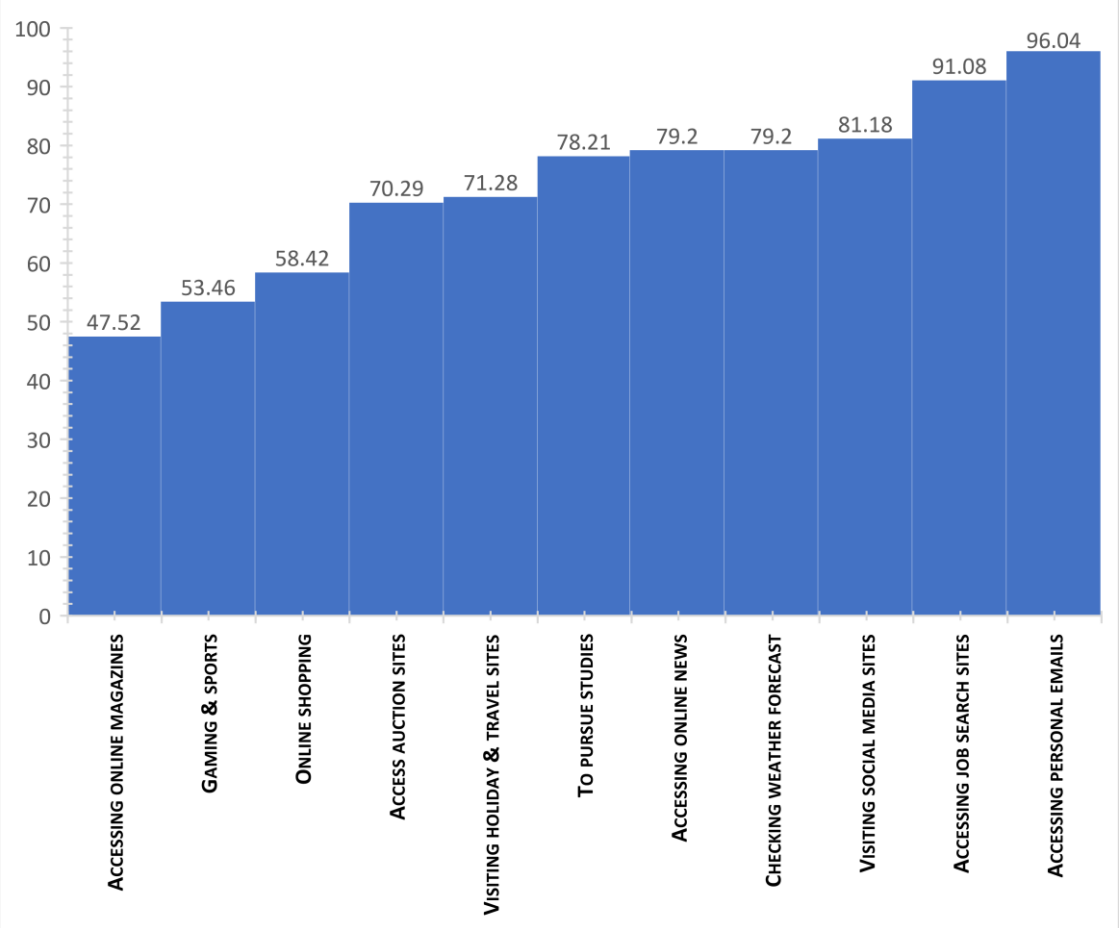


Figure 4. 15 Summary (Cyber-Loafing Activities

4.4.2 Objective 2: To determine tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer care.

This section presents various tools used by managers to control cyber-loafing activities by administrative staff at eThekwini Municipality Sizakala Customer Care . Participants were asked seven questions to measure this objective.

4.4.2.1 Monitoring of the Internet usage

Participants were asked if managers or supervisors were monitoring the Internet usage of workers during working hours. In Figure 4.16, the findings show that 4% strongly agreed with the question, this finding could mean that there are monitoring policies in place, but employees choose not to follow them. The next finding agreed with the statement and rated it at 39.6%. The combined results findings for, “strongly agree” and “agree” findings indicate some level of policy application from the management part. On the other hand, 10.9% “disagreed” with the statement and this finding could be attributed to the fact that staff decided to ignore the implemented policies. The 45.5% of participants being neutral could suggest that participants are not aware of the implemented policies at eThekwini Municipality Sizakala Customer Care. The final bar of (10.9% - “disagree”) in the findings of this question is higher than the first bar (4% - “strongly agree”). These findings are contradictory; an analysis of this is that it could be possible that there are far fewer employees who have remained with the company (who are aware of the policies enforced) since the trend is to search the Internet and access personal e-mail, it is possible that the majority of staff are not aware of the policies enforced within the eThekwini Sizakala Customer Care, while the 10.9% that disagreed, may not even be aware of such policies in place.

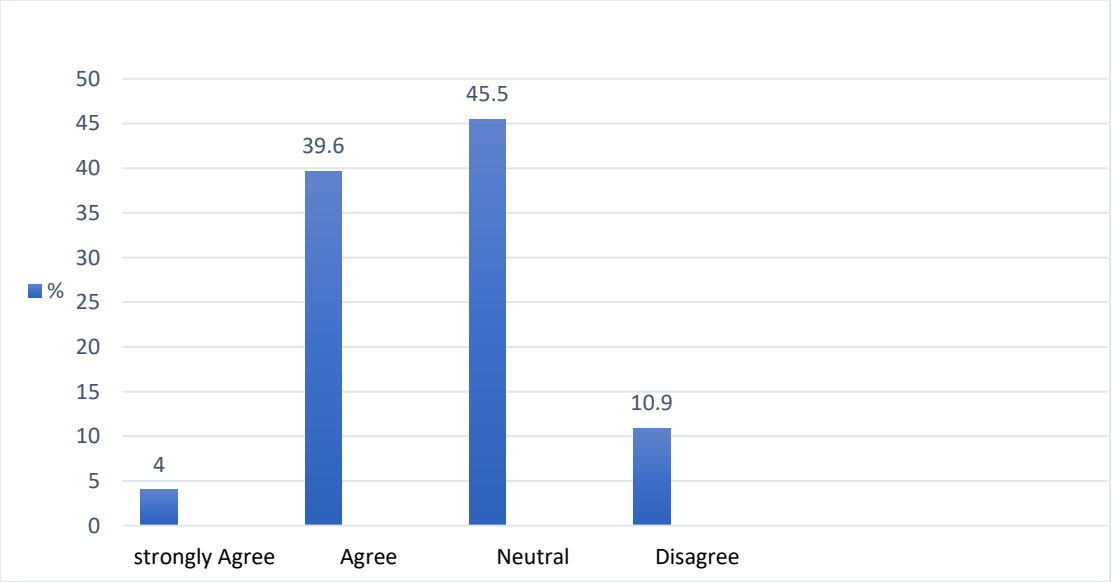


Figure 4. 16 Monitoring of the Internet usage

4.4.2.2 Monitoring software

Participants were asked if the organisation used any monitoring software to retrieve browsing history. As shown in Figure 4.17, 9.9% “strongly agreed”, whilst 58.4% “agreed” that the organisation uses monitoring software to retrieve browsing history. This finding can suggest that managers strive their level best to implement policies within the organisation.

On the other hand, 6.9% “disagreed”, whilst 24.8% were “neutral”. It can therefore be assumed that awareness programmes and workshops regarding monitoring systems are not rigorously enforced at eThekwini Sizakala Customer Care. Such systems keep track of one's history browser, keystrokes and websites visited by employees.

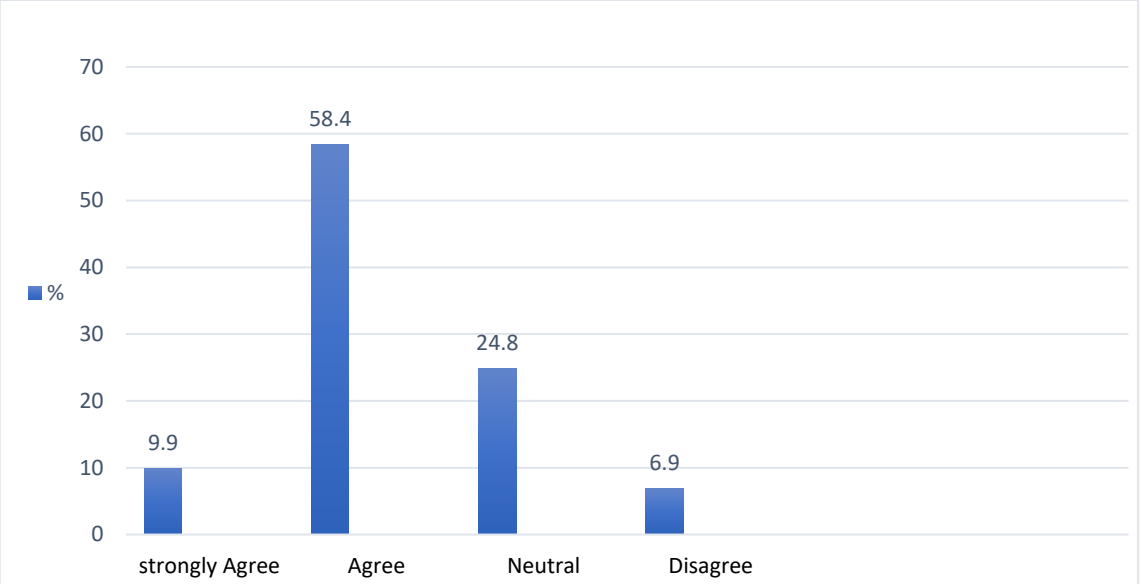


Figure 4. 17 Monitoring software

4.4.2.3 Internet usage policy

The study further asked participants whether the organisation had an internet use policy that guides workers on using the company internet against cyber-loafing activities. As shown in Figure 4.18, the findings reveal that 17.8% of participants “strongly agreed”, whilst 45.5% only “agreed” that the organisation had an internet usage policy. The finding suggests that the policy is in place; it only needs to be enforced. On the other hand, 28.8% were “neutral” and only 7.9% “disagreed”. An internet usage policy is one of the tools at hand to control and monitor internet use at eThekwini Municipality Sizakala Customer Care . In line with this, Soral *et al*. (2020: 65) concur that some organisations have policies to reduce the use of social network sites that negatively affect employee habits and eventually lead to poor productivity. Further, Jandaghi *et al*. (2015: 45) believe that organisational policies that can be put in place negatively or positively influence cyber-loafing and the more transparent the policy, the more it reduces cyber-loafing activities.

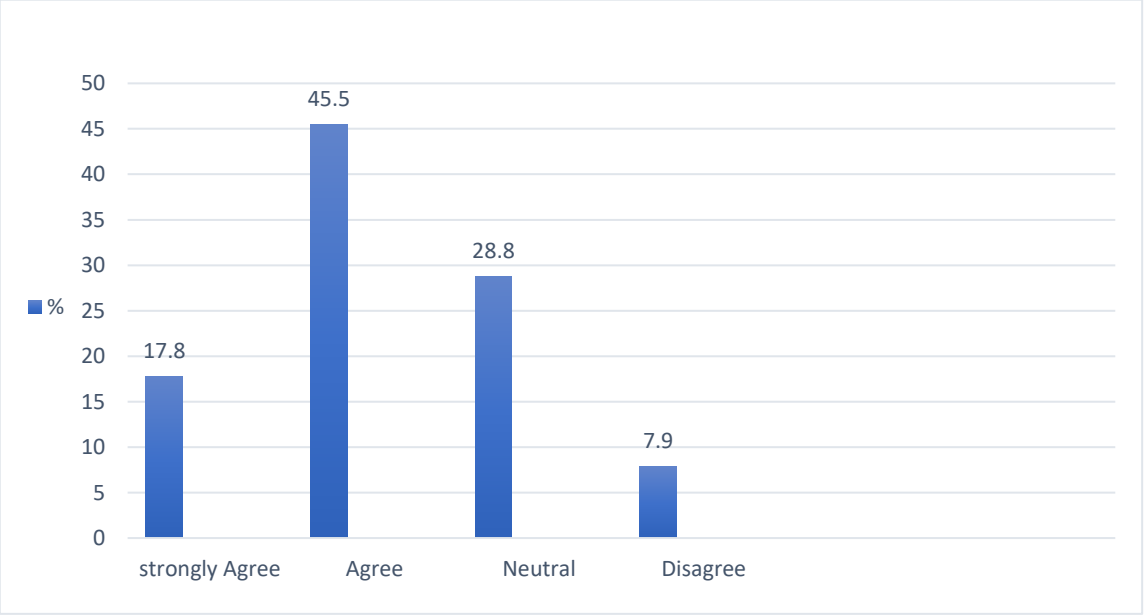


Figure 4. 18 Internet usage policy

4.4.2.4 Implementation and enforcement of internet usage policy

Participants were also asked if managers or supervisors were enforcing the implementation of the Internet usage policy in the organisation. The findings in Figure 4.19 show that 1% of the participants strongly agreed and 27.7% “agreed” that managers or supervisors enforce the implementation of the Internet usage policy in the organisation. On the other hand, 60.4% were “neutral”; this finding of 60.4% could mean that the Internet policy needs to be properly implemented or the Internet usage policy needs to be enforced.

Contrary, 10.9% of the participants “disagreed” that there was enforcement being done on the implementation of the Internet usage policy. It could be possible that staff were not aware such a policy existed. The findings can be supported by Parlier (2019: 39), who reiterated that implementing policies and procedures in organisations of various sizes, is the onus of managers.

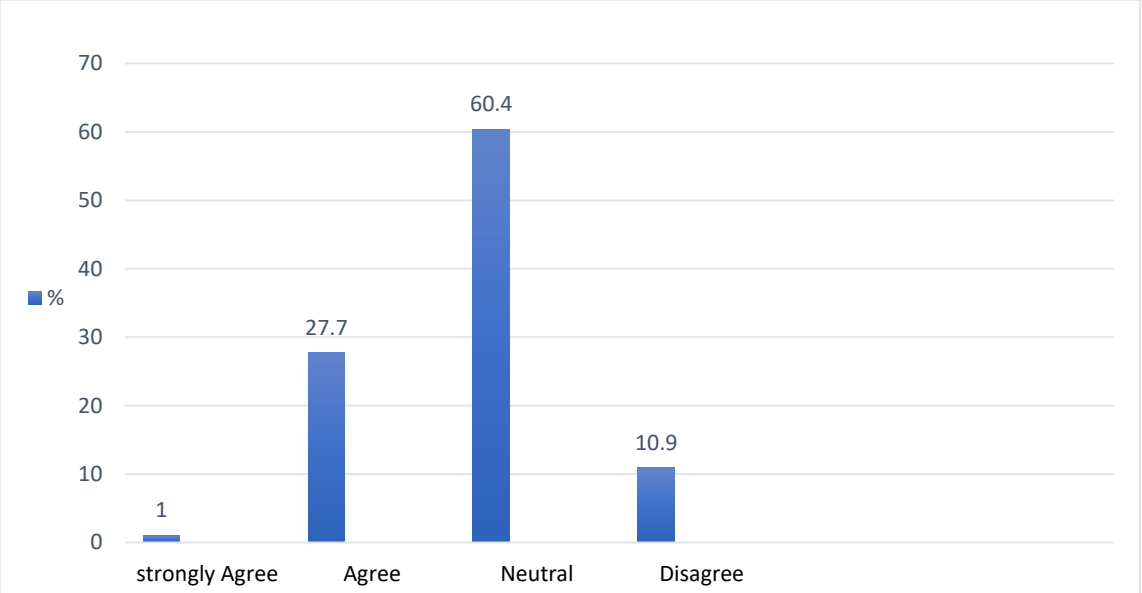


Figure 4. 19 Implementation and enforcement of the Internet usage policy

4.4.2.5 Access blockage to websites

Participants were also asked if they could not access some sites because they had been blocked. Figure 4.20 attempted to ascertain the level at which the organisation had blocked some sites from being accessed by staff and internet users through its IT department. This was confirmed by 25.7% who “strongly agreed” and 34.7% who “agreed” that access to some websites was blocked. Collectively, the "strongly agreed" and "agreed" responses indicated that websites were blocked. On the other hand, 20.8% were “neutral”, 16.8% “disagreed” and 2% “strongly disagreed” with that notion. In confirmation of these findings, Abbasi (2018b) echoed that it is possible for organisations to block sites, monitor e-mails and retrieve browsing history as a measure of preventing cyber-loafing.

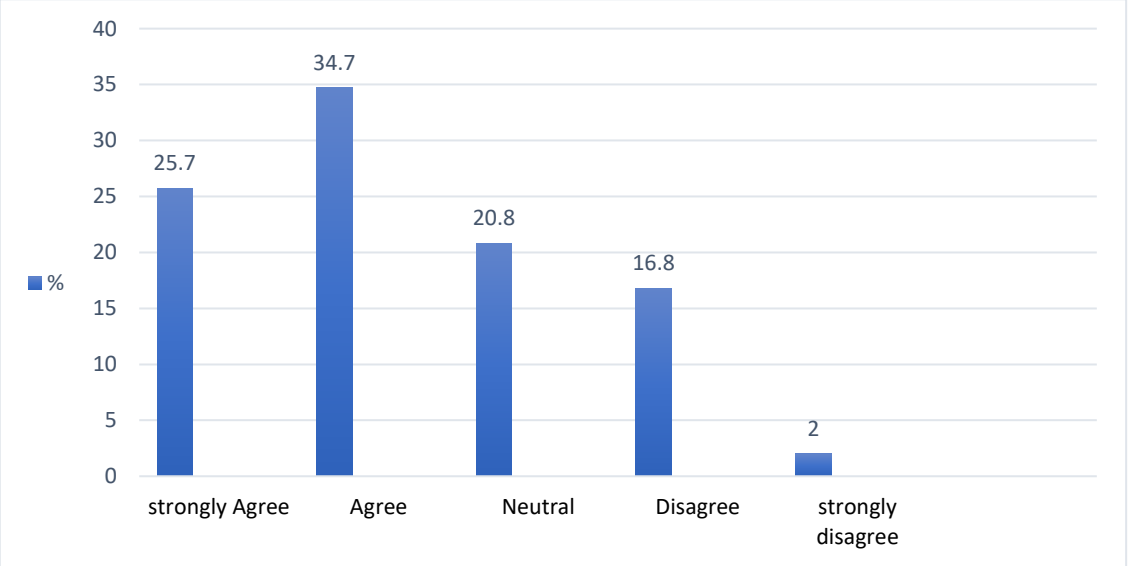


Figure 4. 20 Access blockage to websites

4.4.2.6 Disciplinary action

The findings in Figure 4.21 represent the disciplinary action taken against employees caught using the company and the Internet for personal use. The study findings revealed that 3% “strongly agreed”, whilst 38.6% only “agreed”.

This finding may suggest that disciplinary measures are taken against employees who were found to have transgressed the policy. On the other hand, 45.5% were neutral, 10.9% “disagreed” and 2% “strongly disagreed”. From the findings, disciplinary action is one of the control measures used by managers to prevent cyber-loafing activities. This concurs with Jandaghi *et al.* (2015: 69), who echoed the same sentiment that organisations have continuously warned their employees about the use of the Internet for personal gains and violation of policies on the use of company computers, leading to some employees being dismissed.

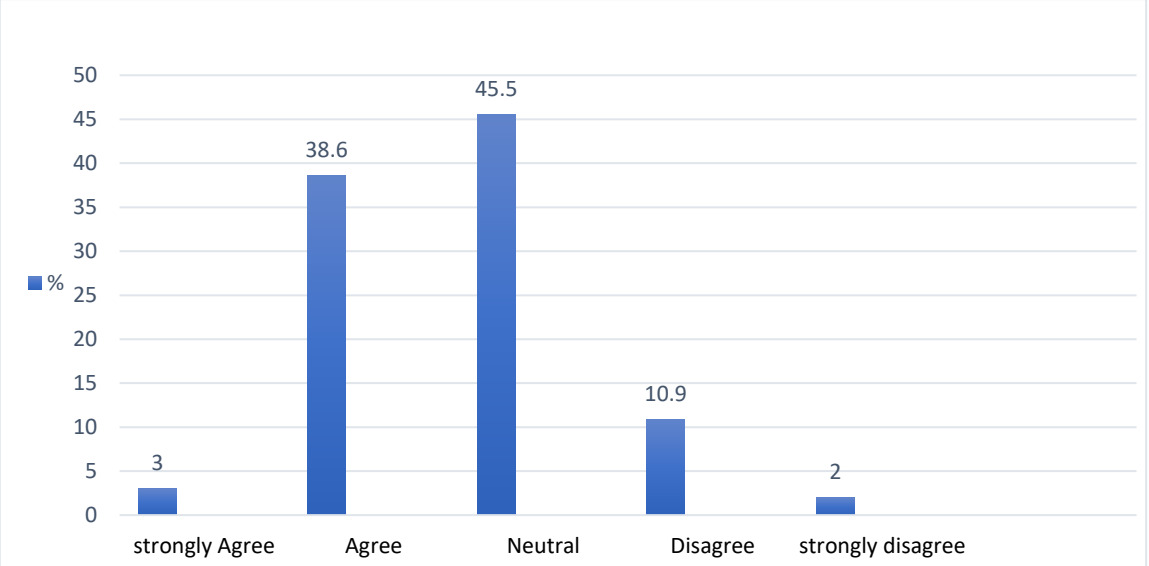


Figure 4. 21 Disciplinary action

4.4.2.7 Communication on the implications of engaging in cyber-loafing

Communication on the implications of engaging in cyber-loafing was one of the questions being asked. The study findings in figure 4.22 indicate that 4% strongly agreed with the statement, whilst 39.6% agreed that continuous awareness of the implications of engaging in cyber-loafing activities was being done. These findings (39.6 and 4% respectively) may suggest that staff was continuously being warned of the implications of such activities. On the other note, 9.9% “disagreed” and 17.8% “strongly disagreed” that there was no communication being done, whilst 28.7% were “neutral”. With the majority in agreement, it can be concluded

that people at eThekwini Sizakala Customer Care know the implications of engaging in cyber-loafing as communication is done.

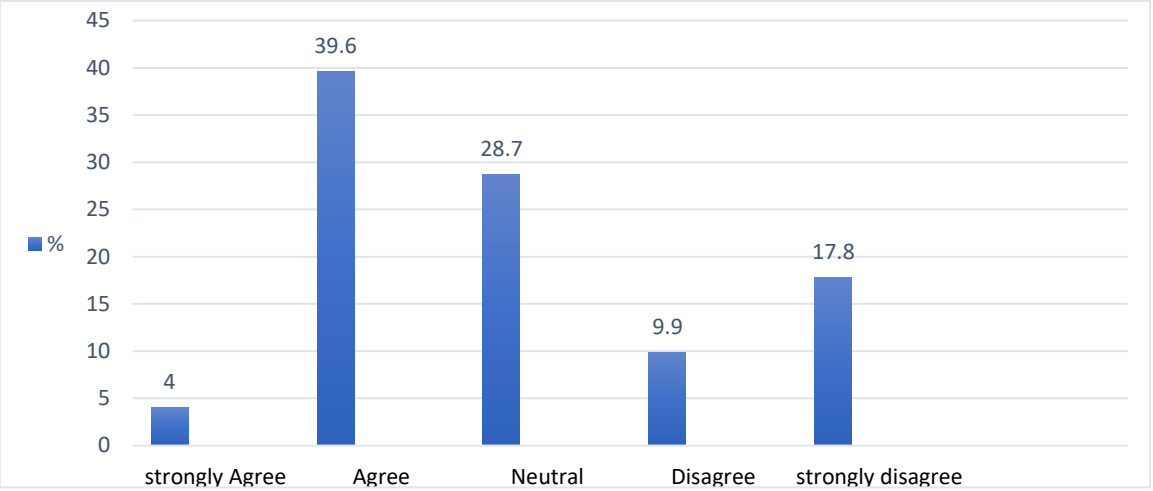


Figure 4. 22 Communication on the implications of engaging in cyber-loafing

4.4.2.8 Conclusion to objective 2

The above section presented and analysed findings from the second objective in determining tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer care. The findings indicated that Managers/supervisors monitor workers' internet usage during work hours. Monitoring software was discovered to be used in the organisation to retrieve browsing history, as confirmed by 68.3% of the participants. Also, the findings reveal that the organisation had an internet use policy that guides workers on using the company internet against cyber-loafing activities. Further to that, findings confirmed that managers or supervisors enforced the implementation of the Internet usage policy in the organisation. The study also found that the organisation blocked some sites, which made it difficult for employees to access during working hours, as confirmed by 60.4%. Furthermore, disciplinary measures were taken against employees caught using the company and the

Internet for personal use and regular communications on the implications of engaging in cyber-loafing activities were done.

4.4.3 Objective 3: To examine factors affecting the implementation of tools that can be used by management to control cyber-loafing by administrative staff in eThekwini Municipality Sizakala Customer Care.

This section presents responses on factors affecting the implementation of tools that can control cyber-loafing activities by administrative staff at eThekwini Municipality Sizakalala Customer Care. The findings are based on six closed-ended questions posed to the participants.

4.4.3.1 Adequacy of Communication from management on internet usage

Participants were asked whether poor communication from management on the Internet usage policy affected the implementation of tools used to control cyber-loafing activities. The findings showed in figure 4.23 that 9.9% strongly agreed, whilst 41.6% only “agreed”. On the other hand, 39.6% were neutral, 7.9% “disagreed” and 1% “strongly disagreed”. Based on the study's findings, with 51% of the participants agreeing, it can allude that communication from management plays a pivotal role in alerting staff on the factors and consequences of cyber-loafing activities.

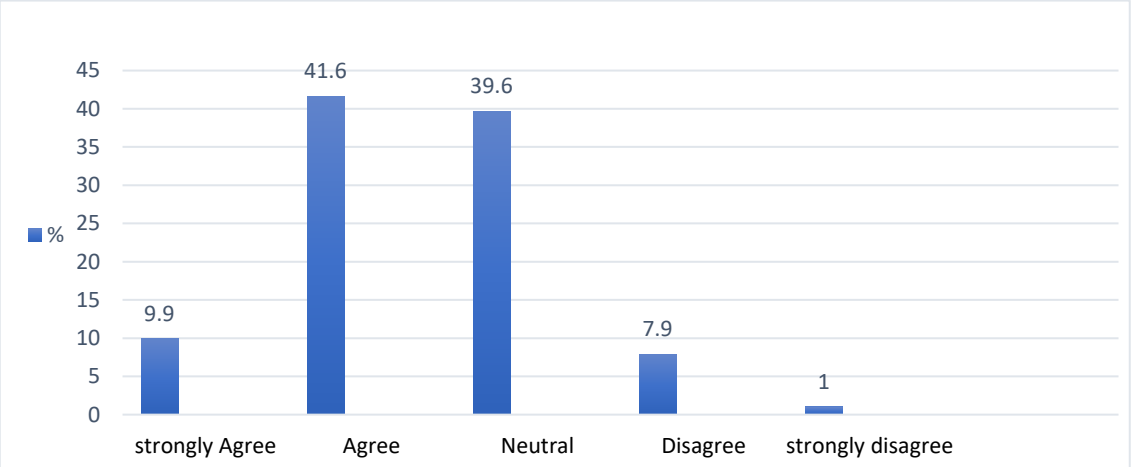


Figure 4. 23 Adequacy of Communication from management on internet usage

4.4.3.2 Workload

The study further asked participants whether their daily workload prevented them from using the Internet for personal use. Figure 4.24 depicts a representation of how questions were answered. Of the participants concerning this question, 24.8% “agreed” that the workload hindered their productivity, whilst 36.6% “disagreed” with this statement. These findings contradict that 24.8% were likely a proportion involved in cyber-loafing activities, whereas the 36.6 who “disagreed” were not involved in cyber-loafing activities. 28.7% of participants were “neutral”; therefore, it can be assumed that they did not want to indicate their working patterns.

On the other hand, 9.9% “strongly disagreed” with the statement, indicating a highly motivated workforce that does not allow their workload to come in the way of their productivity. In light of the majority of participants on the disagreement side, it can be concluded that the administrative staff's workload did not deter them from engaging in cyber-loafing activities. In supporting the above findings, Khan (2021: 85) assert that unmanaged and light workload can lead to cyber-loafing activities.

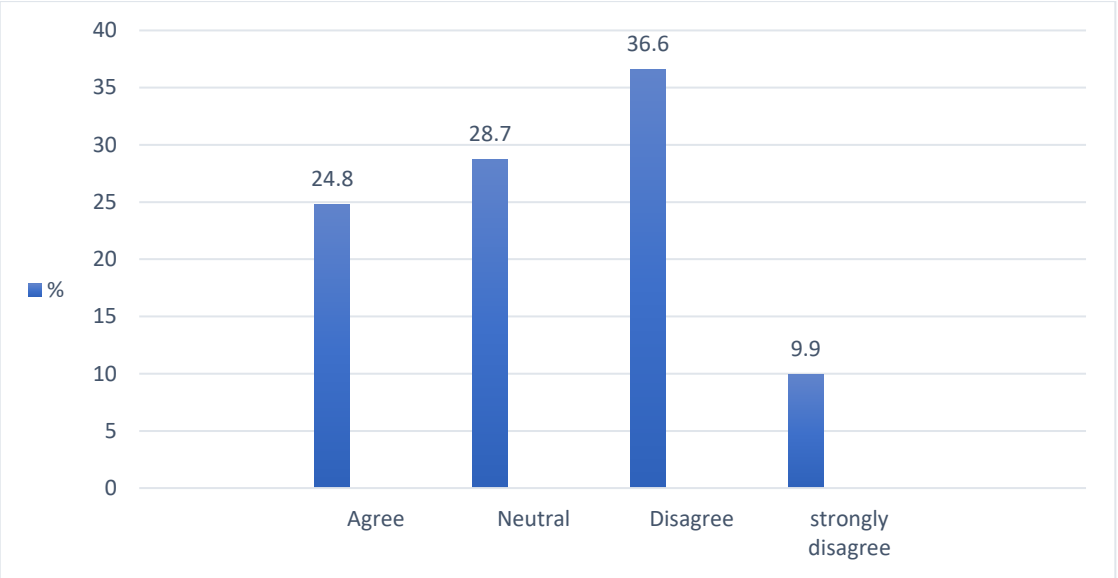


Figure 4. 24 Workload

4.4.3.3 Internet usage monitoring systems

One of the factors affecting the implementation of tools to control cyber-loafing was also posed to participants. Figure 4.25 analysed responses from participants on whether internet usage monitoring systems were another factor affecting the implementation of control systems in preventing cyber-loafing activities. The study revealed that 2% “strongly agreed”, whilst 28.7% only “agreed” that internet usage monitoring systems were another factor affecting the implementation of control systems in preventing cyber-loafing activities. 31.6% were “neutral” 32.7% “disagreed” and 5% “strongly disagreed” that the Internet usage monitoring system is a factor influencing the implementation of control systems in preventing cyber-loafing activities. With most participants not in agreement, the Internet usage monitoring system could be more effective in preventing cyber-loafing activities.

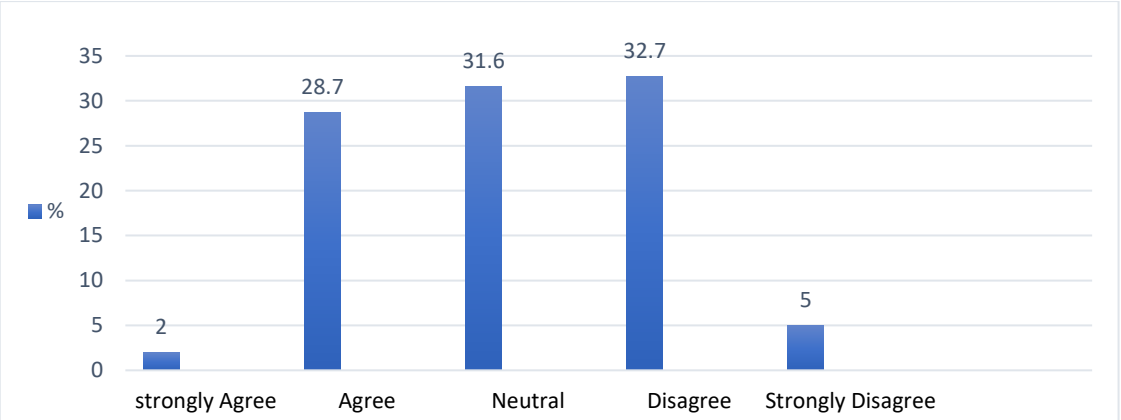


Figure 4. 25 Internet usage monitoring systems

4.4.3.4 The stressful office environment

Figure 4.26 below represents another factor affecting the implementation of tools that can be used to control cyber-loafing activities by administrative staff, as highlighted by participants. From the responses gathered, 15.8% indicated that they strongly agreed, whilst 46.5% only agreed that the stressful environment at the organisation was affecting the implementation of tools that could be used in controlling cyber-loafing activities. On the other hand, 26.8% were neutral, 7.9% disagreed and 3% strongly disagreed that the stressful environment at the organisation was affecting the implementation of tools that could be used in controlling cyber-loafing activities. With the majority of the participants agreeing, it can be concluded that the workplace environment was stressful to the extent that administrative staff engage in cyber-loafing activities. This weakens the effective implementation of tools that could be used in controlling cyber-loafing activities. According to Heath, Sommerfield and von Ungern-Sternberg (2020: 69), a very busy and stressful environment can lead to difficulties in effective policy implementation.

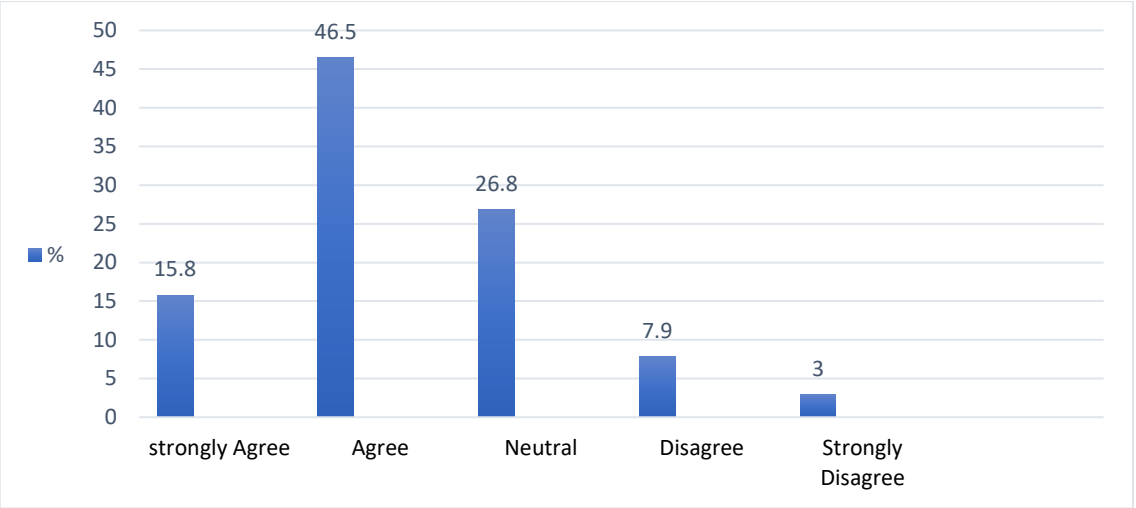


Figure 4. 26 The stressful office environment

4.4.3.5 Organisational culture

Participants were also asked whether organisational culture was another factor affecting the implementation of tools that could be used to control cyber-loafing activities by administrative staff. As depicted in Figure 4.27 below, the study revealed that 20.8% strongly agreed and 40.6% only agreed that organisational culture affected the implementation of tools that could be used to control cyber-loafing activities. On the other hand, 30.7% were neutral, 6.9% disagreed and 1% strongly disagreed with that notion. Based on the findings from the majority who agreed, it can be judged and argued that organisational culture impacts the implementation of various organisational strategies, policies and processes. According to Dubey *et al*. (2017: 54), organisational culture influences various change management initiatives. It can be a bottleneck in policy implementation.

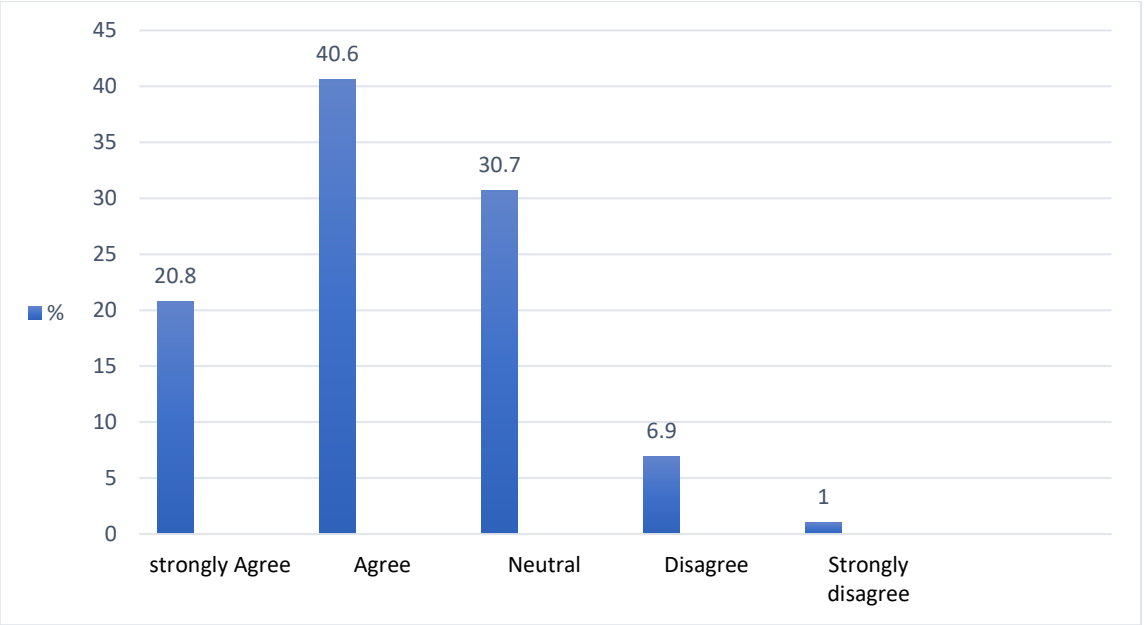


Figure 4. 27 Organisational culture

4.4.3.6 Disciplinary actions

Disciplinary actions taken against staff for transgressing policies were also surveyed by participants in this section. Participants were asked whether the type of disciplinary actions taken against employees for violating internet usage policies affected the implementation of tools that could be used to control cyber-loafing activities by administrative staff. From figure 4.28, the findings highlighted that 4% “strongly agreed” and 23.7% only “agreed” that disciplinary actions against employees violating internet usage policy affected the implementation of tools used to control cyber-loafing activities. The combined responses of “agreed” (23.7%) and strongly “agreed” (4%) indicate that more strategies and disciplinary actions need to be enforced against those found to be in transgression of the implemented policies. On the other hand, the majority, 44.5%, were neutral, 24.8% disagreed and 3% strongly disagreed. The neutral responses (44.5%) may suggest that staff was aware of the policies but chose to ignore them or that the organisation is not forceful enough in taking disciplinary actions against transgressors.

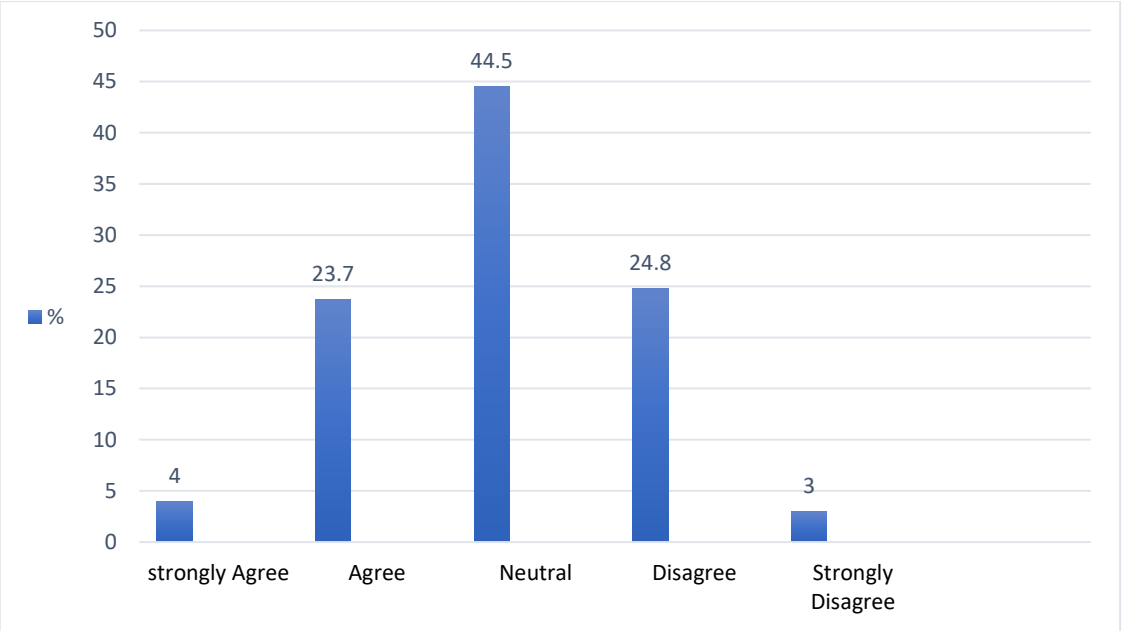


Figure 4. 28 Disciplinary actions

4.4.3.7 Conclusion to objective 3

The data analyses presented findings of objective three on factors affecting the implementation of tools that management can use to control cyber-loafing by administrative staff in eThekwini Municipality Sizakala Customer Care. It emerged from the study that poor communication from management affected the implementation of tools used to control cyber-loafing activities. Moreover, the daily workload was not seen as a prevention mechanism for deterring cyber-loafing activities. In addition, internet usage monitoring systems were not seen as effective in implementing control systems for preventing cyber-loafing activities. The study also concluded that the workplace environment was stressful to the extent that it affected the implementation of tools that could be used to control cyber-loafing activities. Also, organisational culture was concluded to be a significant factor affecting the successful implementation of cyber-loafing tools.

4.5 QUALITATIVE DATA ANALYSIS

This portion of the chapter presents the quantitative data analysis gathered through the open-ended interview questionnaire. Interviews took place from March 2022 to June 2022.

4.5.1 Biographical Information of Management

The analysis begins with the presentation of biographical information of participants, which is shown in Table 4.1 to Table 4.4.

4.5.1.1 Age of participants

Table 4.1 shows the age of participants who completed the semi-structured interview schedule. It is revealed that 36.4% were between 18 and 30 years and 31 and 40 years, respectively. On the other hand, 18.2% were in the age group of 41-50 years and only 9.0% were above 51 years. The findings confirm that most of the managers and supervisors at eThekwini Municipality Sizakala Customer Care were between 18 and 40 years, representing a youthful workforce. The availability of a youthful workforce in an organisation represents a clear future for the organisation.

Table 4. 1 Age of participants

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-30	4	36.4	36.4	36.4
	31-40	4	36.4	36.4	72.7
	41-50	2	18.2	18.2	90.9
	51+	1	9.0	9.0	100.0
	Total	11	100.0	100.0	

4.5.1.2 Gender of participants

Table 4.2 shows the gender distribution of participants, the majority were females, representing 63.6%. On the other hand, 36.4% were male and the findings show that female employees dominated managerial and supervisory positions within eThekwini Municipality Sizakala Customer Care.

Table 4. 2 Gender of participants

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	7	63.6	63.6	63.6
	Male	4	36.4	36.4	100.0
	Total	11	100.0	100.0	

4.5.1.3 Academic level of participants

The study also reviewed the academic level of the participants who took part in the study. Table 4.3 shows that only 36.4% have a matriculation certificate, 18.2% have post-matriculation certificates and another 18.2% have diplomas, whilst 27.3% have degree qualifications. The findings show that the majority of the management has post-secondary school qualifications, indicating that they should have the requisite competency to discharge their responsibilities of curbing cyber-loafing in the workplace.

Table 4. 3 Academic Level of participants

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Matric	4	36.4	36.4	36.4
	Certificate	2	18.2	18.2	54.5
	Diploma	2	18.2	18.2	72.7
	Degree	3	27.2	27.2	100.0
	Total	11	100.0	100.0	

4.5.2 Analysis of objectives per research themes

In dealing with Two themes emerged from the qualitative part of this study, namely cyber-loafing tools and factors affecting their implementation of cyber-loafing tools

4.5.2.1 Theme 1: To identify cyber-loafing activities that are common among administrative staff at eThekwini Municipality Sizakala Customer Care

This section presents qualitative responses based on the second research objective (To identify cyber-loafing activities common among administrative staff at eThekwini Municipality Sizakala Customer Care). The objective was shortened to represent the theme of various questions presented to participants.

Table 4. 4 Monitoring internet usage during working hours

Question 1	How do you monitor employees' internet usage during working hours in eThekwini Municipality Sizakala Customer Care?
Participant	Response
Anonymous 1	"As an employer, it is important to check and monitor the usage of the Internet of my teams to report to my superiors. There is a system put in place currently. Our employees are currently working from home and have been given routers with limited data for a month. Once an employee submits a request for more data during the month, we start monitoring. We give our employees enough data for work a month; that is how we monitor."
Anonymous 2	“We do not check internet usage during working hours. The Computer and Information Technology department sends the report if they pick the misuse of the Internet.”
Anonymous 3	“I monitor internet usage once, during lunchtime.”
Anonymous 4	"It is not a programmed thing, but it is done."
Anonymous 5	“Monitoring is done during working hours.”
Anonymous 6	“The ICT department is in charge of monitoring internet usage.”
Anonymous 7	"Managers do not usually monitor, but the Computer and Information Technology Department monitors through its software to check for any possible violation of their policy."
Anonymous 8	“Sometimes I just come across people using the Internet when l am doing my rounds.”
Anonymous 9	"By moving around, I can identify transgressors."
Anonymous 10	“We do not check it.”
Anonymous 11	"There is no stipulated time, but it is done."

Participants who were managers and supervisors were asked how they monitored internet usage during employees' working hours. The findings in Table 4.4 revealed that there was a need for a consensus on when and how internet usage was monitored. However, Anonymous 1 stated that "*as an employer, it is important to check and monitor the usage of the Internet of my teams to report to my superiors. There is a system put in place currently. Our employees are currently working from home and have been given routers with limited data for a month. Once an employee submits a request for more data during the month, we start monitoring. We give our employees enough data for work a month; that is how we monitor*".

Furthermore, it appears that internet monitoring is a function that is delegated to the Computer and Information Technology Department. This is confirmed by Anonymous 7, who mentioned that "*managers do not usually monitor but the Information Computer Technology department monitors through its software to check for any possible violation of the policy".*

Wang, Liu, Qian and Parker (2021) also believe that organisations use various mechanisms to monitor internet use. Some organisations use internet or desktop surveillance tools to monitor internet use, which the Computer and Information Technology Department largely administers.

Table 4. 5 Reaction to misuse of the Internet

Question 2	How do you react when you walk around and observe administrative staff conducting personal business on their computers at work during working hours?
Participant	Response
Anonymous 1	"It depends on the activity they are doing. I have never been in a situation where I see my employee doing their thing; however, if I were to find myself in that situation, it would depend. If my employee is doing a payment transaction

	(which is easier and time-efficient), I do not think I will have a problem, but if I find my employee watching videos or shopping online, I would have a brief talk with them to call them out of that behaviour."
Anonymous 2	"Administrative staff are aware that they are not allowed to conduct personal business on the company's property. Should they be caught, they will be disciplined and/or dismissed."
Anonymous 3	"I often reprimand them and sometimes query their actions."
Anonymous 4	"They are warned not to engage in private businesses with company machines."
Anonymous 5	"It does not sound nice to see people not doing the work they were employed for."
Anonymous 6	"I will be very angry towards anyone misusing the company resources for personal benefit."
Anonymous 7	"Nothing."
Anonymous 8	"It is not allowed in this organisation."
Anonymous 9	"I will feel somehow furious because a person will not be doing his work."
Anonymous 10	"I will negatively react because what that person will be doing is not accepted."
Anonymous 11	"I do not think there is any reaction; I will do that but will summon the person later."

Concerning the question in Table 4.5 above, participants were further asked how they reacted when they walked around and observed administrative staff conducting personal business on their company computers during working hours. From the responses, it is evident that cyber-loafing is not an acceptable practice. Anonymous 2 and 8 stated clearly that cyber-loafing is not permitted at eThekwini Municipality Sizakala Customer Care. Anonymous 2 mentioned that "*administrative staff are aware that they are not allowed to conduct personal*

business on the company's property. Should they be caught, they will be disciplined and/or dismissed".

Table 4. 6 Internet usage policy

Question 3	Does your organisation have an internet usage policy? If yes, in your opinion, do you think it is adequate to reduce cyber-loafing activities in your organisation?
Participant	Response
Anonymous 1	"Yes, we do have an internet usage policy and it is adequate."
Anonymous 2	"We do not have a system or policy in place at the moment."
Anonymous 3	"Yes, we do have an internet usage policy and it is adequate."
Anonymous 4	"We do have a policy and it is given to every employee who joins the organisation. I do not think it is adequate. After all, once an employee signs the policy, it is put on file because it is something people do not value."
Anonymous 5	"Yes, we do have an internet usage policy and l ensure that employees adhere to it."
Anonymous 6	"The organisation has a policy and it is being followed."
Anonymous 7	"I am not sure if the policy is there because l have not been given it yet."
Anonymous 8	"I am not sure if that policy exists."
Anonymous 9	"Yes, the policy is there, but l do not think it is enough to reduce cyber-loafing."
Anonymous 10	"Yes, but l am not sure if it is enough to prevent the act."
Anonymous 11	"Yes, l do not know what l can say on the policy's adequacy."

The responses gathered in Table 4.6 about the availability of an internet usage policy and its adequateness to reduce cyber-loafing activities in the organisation indicate differing views from the participants. The majority stated that the

organisation had an internet policy; however, its adequacy was being challenged. Anonymous 4, for example, was quoted saying, "*we do have a policy and it is given to every employee who joins the organisation. I do not think it is adequate. After all, once an employee signs the policy, it is put on file because it is something people do not value".*

According to Hadlington and Parsons (2017), not having an internet policy as an organisation in this technology era exposes one or the entire organisation to cyber risks. However, in a study by Rahimnia and Karimi-Mazidi (2015: 69), only 40% of managers believed that the Internet policy was sufficient for deterring cyber-loafing. This means that managers must largely place more value on the Internet policy as a cyber-loafing deterrence.

Table 4. 7 Communication of internet usage policy

Question 4	Do you think the Internet usage policy is clearly articulated and communicated within the organisation?
Participant	Response
Anonymous 1	“No, it is not. The number of employees who submit requests for data during the month increase monthly.”
Anonymous 2	“Annually, the organisation offers online Code of Business Conduct and Ethics training to existing and new employees.”
Anonymous 3	“Yes, the policy is well communicated and implemented.”
Anonymous 4	“I think it is well articulated because most people are aware of the consequences of playing on the Internet with company computers.”
Anonymous 5	“The policy is well articulated and communication is always provided to new employees.”
Anonymous 6	“Yes, the policy is well articulated and communicated at all levels.”
Anonymous 7	“The Computer and Information Technology department frequently sends communications to us concerning this issue. It is well-articulated I guess.”
Anonymous 8	“The policy is well articulate, yes.”
Anonymous 9	“As for me, I would not say it is well communicated. I am not sure.”
Anonymous 10	“Not really!! Or maybe I have not come across the communication.”
Anonymous 11	“Yeah! The policy is well-articulated.”

Table 4.7 indicates that most participants agreed that the Internet usage policy was clearly articulated and communicated within the organisation. The responses showed that the Internet policy needed to be better shared amongst staff. As highlighted by Anonymous 2 “*Annually, the organisation offers online Code of Business Conduct and Ethics training to existing and new employees*”.

Anonymous 3 further said, "*Yes, the policy is well communicated and implemented".* Anonymous 4 said, *"I think it is well articulated because most people are aware of the consequences of playing on the Internet with company computers".* This is despite Anonymous 7's response, indicated that the Computer and Information Technology Department frequently circulates the Internet policy to staff as he/she was quoted saying *"the Computer and Information Technology Department frequently sends communications to us concerning this issue. It is well articulated, I guess*.

Given the above finding, Abubakar and Al-zyoud (2021: 36) are also of the view that it is essential to keep informing employees of any policies and procedures that their company uses, as well as requiring them to formally acknowledge that they have received the communiqué each time it is circulated. This is the only legally sound way to hold them accountable for the new policies and procedures that have been implemented.

Table 4. 8 Enforcement & implementation of internet usage policy

Question 5	How is the Internet usage policy enforced and implemented in your organisation?
Participant	Response
Anonymous 1	"Internet usage is not one of the factors that we tend to focus on. Once an employee submits the request for more data, we process the data and should the person continue finishing their date before month end in three consecutive months, we then take measures in enforcing policies to that employee not the organisation as a whole."
Anonymous 2	"Through training and e-mails."
Anonymous 3	"In the form of writing or verbal communique. Mechanisms are put in place to ensure policy implementation effectively."
Anonymous 4	"The policy is enforced and implemented in writing."

Question 5	How is the Internet usage policy enforced and implemented in your organisation?
Participant	Response
Anonymous 5	"We always receive e-mails reminding us of cyber threats from the Computer and Information Technology Department."
Anonymous 6	“I am not sure about this one.”
Anonymous 7	“Sometimes people are monitored online and reprimanded for abusing the Internet.”
Anonymous 8	“We have seen some websites being blocked, so l guess that is how the organisation is enforcing compliance with its Computer and Information Technology usage policy.”
Anonymous 9	“People are trained first and made to sign the usage policy.”
Anonymous 10	“I do not exactly know how this is done or maybe l have not come across such an exercise.”
Anonymous 11	“The policy is communicated to people.”

Further, from the structured interview responses in Table 4.8 above. Participants were also asked how their organisation enforced and implemented the Internet usage policy. From the quantitative question, several participants needed to figure out how the internet usage policy was implemented and enforced. However, responses from the interviewed participants revealed a different scenario. For example, Anonymous 1 said, “*Internet usage is not one of the factors that we tend to focus on. Once an employee submits the request for more data, we process it and should the person continue finishing their date before month end in three consecutive months. We then take measures in enforcing policies on that employee, not the organisation as a whole.”*

Anonymous 2 said, *“through training and e-mails"* and anonymous 5 said, “*we always receive e-mails reminding us of cyber threats from the Computer and Information Technology department."* Whilst Anonymous 3 was quoted saying, *“monitoring was done in form of writing or verbal communique,”* Anonymous 7

said, *"sometimes people are monitored online and reprimanded for abusing the Internet."*

Anonymous 8 said, "*we have seen some websites being blocked, so I guess that is how the organisation is enforcing compliance with its Computer and Information Technology usage policy*". Anonymous 9 said, "*people are trained first and made to sign the usage policy*". Anonymous 10 was also quoted saying, "*I do not exactly know how this is done or maybe I have not come across such an exercise".* Anonymous 11 said, *"the policy is communicated to people"*

Table 4. 9 Awareness programmes

Question 6	Does your organisation conduct awareness programmes or training on the risks and dangers of cyber-loafing? If yes, how effective are these programmes?
Participant	Response
Anonymous 1	"Yes, we do conduct awareness and training. They are very effective."
Anonymous 2	"There has never been a programme specifically for cyber-loafing, simply because we trust our employees to do the right thing all the time."
Anonymous 3	"Yes, we do such programmes at least twice a year."
Anonymous 4	"I am not sure I have not come across any campaign or awareness."
Anonymous 5	"Not really because they don't sound like awareness programmes."
Anonymous 6	"I would not say they are not there; they happen once in a blue moon and their effectiveness could be clearer.
Anonymous 7	"It is a tricky one. I would not say much."
Anonymous 8	"We have not received any form of training on Cybers-loafing."
Anonymous 9	No. I have not come across such programmes."

Question 6	Does your organisation conduct awareness programmes or training on the risks and dangers of cyber-loafing? If yes, how effective are these programmes?
Participant	Response
Anonymous 10	“I am not very sure.”
Anonymous 11	"These programmes used to be done a long time ago when the use of computers began to flood."

In addition to the responses in Table 4.9, managers and supervisors were also asked whether the organisation conducts awareness programmes or training on the risks and dangers of cyber-loafing and how effective these programmes were. The findings revealed that employees needed to be fully aware of any continuous awareness programmes on cyber-loafing activities, both from the administrative staff above and from management or supervisors.

For instance, this can be confirmed by Anonymous 2, who said, “*there has never been a programme specifically for cyber-loafing, simply because we trust our employees to do the right thing all the time”*. Anonymous 8 said, “*we have not received any form of training on Cyber-loafing”*. and Anonymous 9 outrightly said, “*no, I have not come across such programmes*". On the other note, some participants were unsure, as confirmed by Anonymous 4, who said, *“I am not sure, I have not come across any campaign or awareness”,* and Anonymous 5, *“not really because they do not sound like awareness programmes”* Anonymous 7 said, *“it is a tricky one. I would not say much”.* Anonymous 10 said, *“I am not very sure*”. In support of the above findings, management's mechanism as a preventive strategy to curb cyber-loafing activities is continuous training in behaviour among employees (Kasap 2019: 66). Employees need to be continuously educated about various cyber threats and the negative consequences of engaging in cyber-loafing activities. According to Hadlington and Parsons (2017: 55), a positive relationship exists between cyber-loafing activities and poor internet security awareness. There is a need to train managers

and supervisors on cyber security issues so that they can advise their subordinates.

Blocking of websites

Question 7	What are your views on blocking websites as a strategy and a way of mitigating cyber-loafing activities?
Participant	Response
Anonymous 1	“There should be sites blocked. For example, on YouTube, Employees may want to watch videos even during their lunch break. Those videos may lead to time and data consumption.”
Anonymous 2	“No, I do not think it will be an effective way forward. Employees need discipline.”
Anonymous 3	“It is the most effective way of mitigating cyber-loafing activities and it’s used by most advanced institutions nationwide.”
Anonymous 4	“It is the best way to prevent the waste of resources.”
Anonymous 5	“I think it is a commendable effort because you will not have trouble with any person on the Internet.”
Anonymous 6	“It is a good strategy.”
Anonymous 7	“I think it is good to block some websites like social media.”
Anonymous 8	“It is a good strategy; people are playing around with the Internet and it’s costing the company a lot of money.”
Anonymous 9	“Blocking websites is a good strategy.”
Anonymous 10	“It is a good strategy I think.”
Anonymous 11	“It is one of the effective strategies in dealing with cyber loafers.”

Table 4.10 above depicts responses from managers and supervisors regarding their views on blocking websites as a strategy and a way of mitigating cyber-loafing activities. From the findings, all participants confirmed that blocking

websites was a good strategy for mitigating cyber-loafing activities. In light of this, anonymous 1 said, "*there should be sites blocked. For example, YouTube, Employees may want to watch videos even during their lunch break. Those videos may lead to time and data consumption".* Anonymous 3 said, *"it is the most effective way of mitigating cyber-loafing activities and it is used by most advanced institutions nationwide".* Anonymous 4 said, "*it is the best way to prevent the waste of resources".* Anonymous 5 commented, *"I think it is a commendable effort because you will not have trouble with any person on the Internet"* .Anonymous 8 added, *"it is a good strategy; people are playing around with the Internet and it is costing the company money".*

In line with the above findings, Lim and Tee (2021: 69) said that the leaders of organisations must embrace monitoring and security techniques such as the blocking of websites, the tracking of e-mails and the examining of browser histories. Alharthi (2018: 106) further confirmed that to combat cyberslacking, several companies have implemented multiple regulations and preventative measures, such as mobile compartments, restricting websites and providing reminders to employees.

Table 4. 10 Electronic monitoring systems

Question 8	Are electronic monitoring systems used in your organisation to block employees from accessing certain websites? How effective are they?
Participant	Response
Anonymous 1	"Yes, there are electronic systems that are effectively monitored."
Anonymous 2	"Yes, there are. As explained in the answer above, our employees are blocked from accessing YouTube and we find that strategy effective."
Anonymous 3	"Yes. I have come across them."
Anonymous 4	"The electronic monitoring systems are there."

Question 8	Are electronic monitoring systems used in your organisation to block employees from accessing certain websites? How effective are they?
Participant	Response
Anonymous 5	“Yes. They are there and they seem to be good.”
Anonymous 6	“Yes, and regarding their effectiveness, I think it is effective.”
Anonymous 7	“I do not know, I have not heard of such a monitoring system.”
Anonymous 8	“I think that would need the Computer and Information Technology to depart, they are the one who knows about monitoring systems.”
Anonymous 9	“I am not sure if these systems are in place.”
Anonymous 10	“I think the Computer and Information Technology department would know much better on this because I have not been shown any.”
Anonymous 11	“The systems are there.”

In Table 4.11, supervisors and managers were asked if electronic monitoring systems were used to block employees from accessing certain websites. The majority confirmed that electronic monitoring systems were used in the organisation to block employees from accessing certain websites. This was confirmed by anonymous 1, who said, *“yes, there are electronic systems that are effectively monitored”*, and Anonymous 2, who said, *“yes, there are”. As explained in the answer above, “our employees are blocked from accessing YouTube and we find that strategy effective”. Anonymous 3 said, “yes. I have come across them”*. Anonymous 6 said, “*yes and regarding their effectiveness, I think it is effective”*. On the other note, anonymous 7 and 8 were not sure, respectively, as they said, “*I don’t know, I have not heard of such monitoring system”,* and “*I am not sure if these systems are in place”.* To confirm the above findings, Alharthi (2018: 88) highlighted that one efficient strategy for lowering the amount of time

spent cyber-loafing is to implement operant conditioning with software that filters the Internet and monitors user activity.

Table 4. 11 Informed on internet abuse

Question 9	Have you ever been formally informed about the abuse of the Internet and computer usage by the employee? If yes, what was the disciplinary procedure that was followed?
Participant	Response
Anonymous 1	“I have never been in a formal disciplinary hearing with an employee regarding the abuse of the Internet.”
Anonymous 2	“No, I have not; however, Human Resources Department takes care of that part should it happens.”
Anonymous 3	“No. Not really.”
Anonymous 4	“No, maybe they are covering each other”
Anonymous 5	“No one has approached me or to report any form of abuse.”
Anonymous 6	“People are protecting each other; you will never see any person reporting another person.”
Anonymous 7	“No. I have not been informed of any internet abuse.”
Anonymous 8	“No. no one has ever come to me to report someone. “
Anonymous 9	“It is very tricky and very rare to see a person reporting someone. If that reporter is known, it might cause tension between the people.”
Anonymous 10	“No one has reported.”
Anonymous 11	"I have never seen anyone reporting on such issues before. I think they are covering for each other."

To further strengthen qualitative findings, the structured interview included a question directed to managers and supervisors on whether disciplinary action had once been taken against an employee for abusing internet and computer usage and whether disciplinary action was taken. From the above findings in Table 4.12, this was the first time anyone had encountered such a situation based on the responses. However, it confirmed that disciplinary measures could be taken if such a case happened. For instance, Anonymous 1 said, *"I have never been in a formal disciplinary hearing with an employee regarding the abuse of the Internet".* Anonymous 2 said, "*no, I have not; however, Human Resources Department takes care of that part should it happens". Anonymous 5 said, "no one has approached me or reported any form of abuse".* Anonymous 6 said, "*people are protecting each other; you will never see any person reporting another person".* Anonymous 9 said, "*it is very tricky and very rare to see a person reporting someone. If that reporter is known, it might cause tension between the people*". Moreover, Anonymous 11 said, *"I have never seen anyone reporting on such issues before. I think they are covering for each other".*

Perceived certainty and severity of possible cyber-loafing punishments were found to mitigate the impact of observability on employee cyber-loafing. Once employees understand that there are punishment protocols for violating organisational policies, they will refrain from committing unacceptable and deviant behaviours (Piscotty, Martindell and Karim 2016: 107).

4.5.1.2 Conclusions on Theme 1

Theme one presented cyber-loafing activities common among administrative staff at eThekwini Municipality Sizakala Customer Care. The findings revealed that managers had strategies to curb cyber-loafing activities. Some units had this duty performed by the Information Technology Department. Some managers confirmed that they would walk around supervising their employees and checking their internet usage whenever they had time. In the process of monitoring, the findings concluded that managers would not respond leniently towards those

violating the Internet policy as they further confirmed that the organisation had an internet usage policy in place. It can also be concluded that the Internet usage policy was clearly articulated and communicated within the organisation. Employees needed to be fully aware of continuous awareness programmes on cyber-loafing activities, both from the administrative staff above and from management or supervisors. However, the blocking of internet sites as a strategy for preventing cyber-loafing was well received by participants.

4.5.2.3 Theme 2: To determine tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer care.

This section presents qualitative responses based on the third research objective (to examine factors affecting the implementation of tools managers can use to control cyber-loafing by administrative staff in eThekwini Municipality Sizakala Customer Care). The objective was shortened to represent a theme of various questions presented to participants.

Table 4. 12 Daily workload

Question 1	Do you think that the daily workload that is distributed to the employees is enough to keep them throughout the day working without cyber-loafing?
Participant	Response
Anonymous 1	“Yes, that is why we look at employees' results when they start using more data.”
Anonymous 2	“Yes, work is enough for the day; sometimes, working hours are not enough to complete.”
Anonymous 3	“Yes! The workload is sufficient to keep the employee busy throughout the day.”
Anonymous 4	“I guess the workload is enough to keep employees busy.”

Anonymous 5	“The workload is more than enough to keep them busy throughout the day.”
Anonymous 6	“Yes, people will not have time to play around with the Internet and social media.”
Anonymous 7	“Yes, the workload is enough.”
Anonymous 8	“I believe so, it is enough to keep them occupied with work.”
Anonymous 9	“Yes, the daily workload that is distributed to the employees is enough to keep them throughout the day working without cyber-loafing.”
Anonymous 10	“I think so because they will not have time to play around.”
Anonymous 11	“I think giving employees a workload always keeps them busy and off the Internet to play.”

From the interviews, a related question was presented to managers and supervisors on whether the daily workload distributed to the employees was enough to keep them working throughout the day without cyber-loafing. Table 4.13 above shows that employees sometimes do not have time or have limited time to engage in cyber-loafing due to workload and pressure. This was witnessed by all participants, who confirmed that the daily workload distributed to the employees is enough to keep them working throughout the day without cyber-loafing. For example, Anonymous 1 said, “*yes, that is why we look at employees' results when they start using more data*”. Anonymous 2 said, “*yes, work is enough for the day; sometimes, working hours are not enough to complete”*. Anonymous 3 said, ‘*yes! The workload is sufficient to keep the employee busy throughout the day”.* Anonymous 5 said, “*the workload is more than enough to keep them busy throughout the day”.* Anonymous 9 said, *“yes, the daily workload that is distributed to the employees is enough to keep them throughout the day working without cyber-loafing*”. However, in light of the above findings, Aladwan, Al Muala and Salleh (2021: 99) found that studies have shown that workload affects

organisational commitment and leads to employees evading their work and duties and in the end, partaking in personal activities.

Table 4. 13 Work facility conditions

Question 2	Are your work facility conditions influencing employees to engage in cyber-loafing activities?
Participant	Response
Anonymous 1	“No, all our employees have internet access, limited access and some webs are blocked, but everyone has internet access.”
Anonymous 2	“No, we are an FMCG processing plant; pressure is always there. There is not much time to engage in cyber-loafing.”
Anonymous 3	“No, it is a busy environment.”
Anonymous 4	“No, they do not influence such behaviour.”
Anonymous 5	“I do not think so, because people are always busy with their work.”
Anonymous 6	“Not really, I have not seen such.”
Anonymous 7	“No, the environment does not influence employees to engage in cyber-loafing activities.”
Anonymous 8	“The environment does not influence employees to engage in cyber-loafing activities.”
Anonymous 9	“Not that much.”
Anonymous 10	“I do not believe so, if it was influencing, we could be experiencing a lot of cyber-loafing activities."
Anonymous 11	“The environment does not influence employees to engage in cyber-loafing activities.”

In addition to the quantitative findings, managers and supervisors were asked to answer an interview question enquiring whether work facility conditions influence employees engagement in cyber-loafing activities. According to Table 4.14 above, participants disagreed that the work facility conditions influenced

employees to engage in cyber-loafing activities. This was confirmed, for instance, by Anonymous 1, who said, "*no, all our employees have internet access, limited access and some webs are blocked, but everyone has internet access".* Anonymous 2 said, "*no, we are an FMCG processing plant; pressure is always there*." Further, anonymous 4 said, "*no, they do not influence such behaviour."* Anonymous 7 said, "*no, the environment does not influence employees to engage in cyber-loafing activities"*. Anonymous 8 said, "*the environment does not influence employees to engage in cyber-loafing activities"*. Anonymous 10 commented "*I do not believe so. If it was influencing, we could be experiencing a lot of cyber-loafing activities".* Anonymous 11 said, "*the environment does not influence employees to engage in cyber-loafing activities".* According to Prakash and Kaur (2018: 33), employees who view their work as monotonous due to a lack of opportunities to learn new things or use their talents are more likely to engage in cyber-loafing.

Table 4. 14 The rise in virtual work

Question 3	Do you think the rise in virtual work influences employees to cyber-loafing?
Participant	Response
Anonymous 1	"It depends on the employee's individual. Some employees do not want to go back to the office and they will do anything not to go back; one of those things is to use the Internet wisely and for work-related things only."
Anonymous 2	"Yes, it should not be, but it does. Working from home tends to be more relaxing and comfortable as compared to the workplace. You have plenty of time to do your activities."
Anonymous 3	"Yes, the rise in virtual work influences employees to cyber-loafing."
Anonymous 4	"The rise in virtual work influences employees to cyber-loafing."
Anonymous 5	"Yes, virtual work influences employees to cyber-loafing."

Anonymous 6	“Yes, I witnessed that during the Covid-19 era.”
Anonymous 7	“I think so because no one will be monitoring you, so people with have ample time to access anything they want.”
Anonymous 8	“Yes, virtual work influences employees to cyber-loafing.”
Anonymous 9	“Yes, people were cyber-loafing during Covid.”
Anonymous 10	“Yes. Virtual work needs people who are mature enough.”
Anonymous 11	“I think so because no one will be monitoring.”

On the other hand, the shift to virtual working because of COVID-19 can lead to some employees seeing working from home as stressful. Another related question to the stressful environment was whether managers and supervisors think the rise in virtual work influences employees to cyber loaf. As depicted in Table 4.15, all participants agreed that the rise in virtual work had influenced employees to cyber-loafing as depicted in a few responses, Anonymous 1 said*, “it depends on the employee's individual. Some employees do not want to return to the office and will do anything not to go back; one of those things is to use the Internet wisely and for work-related things only”*. Anonymous 2 said, *ÿes, it should not be, but it does. Working from home tends to be more relaxing and comfortable compared to the workplace. You have plenty of time to do your activities”.*

Furthermore, Anonymous 3 said, *“yes, the rise in virtual work influences employees to cyber-loafing”.* Anonymous 7 said, *"I think so because no one will be monitoring you, so people have ample time to access anything they want”.* Concurring with the above findings, Ezeh, Etodike and Chukwura (2018: 96) narrated that opportunities for cyber-loafing, or using the Internet for activities that are not related to one's job, have increased significantly in recent years as a result of the proliferation of virtual work teams, flexible work arrangements and personal electronic devices in the workplace. This has led to a significant increase in the number of challenges faced by many firms.

Table 4. 15 Organisational culture

Question 4	Does your organisational culture encourage or lead to cyber-loafing by administrative staff?
Participant	Response
Anonymous 1	"We encourage a healthy environment where employees need to produce 100% results. I do not think our organisational culture does encourage cyber -loafing."
Anonymous 2	"No. organisational culture does not influence cyber-loafing."
Anonymous 3	“No. our organisational culture is a different one.”
Anonymous 4	“I do not think so.”
Anonymous 5	“No. our organisation does not allow misuse of company resources.”
Anonymous 6	“I do not think organisational culture encourages or leads to cyber-loafing.”
Anonymous 7	“We have a good culture that does not tolerate such behaviour.”
Anonymous 8	“I do not know about the culture, but what I can say is cyber--loafing is not tolerated.”
Anonymous 9	"The organisation does not have such type of culture. We have a culture of hard-working."
Anonymous 10	“No I do not think culture encourages such activities. The culture in this organisation seems to be solid from the top. If the top management were cyber loafers, that could have scaled down.”
Anonymous 11	"The culture in this organisation is not like that."

In addition to the quantitative findings and qualitative, questions enquired if the organisational culture encourages or leads to cyber-loafing by administrative staff. All participants highlighted that the organisational culture was not one of those that encouraged cyber-loafing. As confirmed by several participants,

Anonymous 1 said, "*we encourage a healthy environment where employees must produce 100% results. I do not think our organisational culture does encourage cyber- loafing"*. Anonymous 2 said, *"no. organisational culture does not influence cyber-loafing*". Anonymous 5 said, "*no. our organisation does not allow misuse of company resources"*. Anonymous 9 said, "*the organisation does not have such type of culture. We have a culture of hard-working. … No, I do not think culture encourages such activities"*. Anonymous 10 said, "*the culture in this organisation seems to be solid from the top. If the top management were cyber loafers, that could have scaled down".* This confirms that the organisation's strong culture does not tolerate deviant behaviour.

4.5.1.4 Conclusion on Theme 2

In conclusion, theme 2 investigated the tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer Care. It is concluded that management uses workload to prevent cyber-loafing activities. It was also reported that the work facility conditions not to influence employees to engage in cyber-loafing activities. However, with the rise of virtual working conditions, it was noted that the conditions could influence employees to engage in cyber-loafing activities. In determining the effectiveness of organisational culture, the findings concluded that the current organisational culture did not encourage cyber-loafing by administrative staff.

4.6 CONCLUSION

The main purpose of the above chapter was to present data collected through closed-ended questionnaires and an open-ended interview schedule. The chapter presented various cyber-loafing activities that were common among the administrative staff of eThekwini Municipality Sizakala Customer Care. Such activities included online shopping, gaming and sports; visiting holiday and travel sites and social media sites; accessing job search sites, online news, online magazines, auction sites, and accessing personal e-mails; checking weather

forecasts; and doing studies. Tools used by managers to control cyber-loafing activities by administrative staff were also presented, as were factors affecting the successful implementation of those tools. The next chapter presents the overall conclusion and recommendations for the study.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

In this chapter, the study's overall conclusion is given, linking the aim with objectives of the study and empirical and theoretical assessment. The chapter offers a summary of the key findings of this study and presents how the research objectives were achieved. Furthermore, this chapter discusses the theoretical and practical implications of this research study and the recommendations arising from the findings and suggestions for further research on the area of study.

5.2 OVERVIEW OF THE STUDY

This study's main aim was to evaluate existing tools used by managers to prevent and control cyber-loafing by administrative staff in the workplace using the case study of eThekwini Municipality Sizakala Customer Care. To achieve this aim, the following objectives were formulated:

- To identify cyber-loafing activities that are common among administrative staff at eThekwini Municipality Sizakala Customer Care.
- To determine tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer Care.
- To examine factors affecting the implementation of tools that can be used by management to control cyber-loafing by administrative staff in eThekwini Municipality Sizakala Customer Care.

The literature review in Chapter 2 presented a comprehensive discourse on cyber-loafing challenges and the available tools that are used to deter employees from this malpractice. This study focused on employees who engage in non-work-related activities or use the computer and internet for personal purposes.

Common cyber-loafing activities were identified and discussed and these include online shopping, social networking, gambling and sending personal emails, among others (Jandagh *et al.* 2015: 35). The identification of cyber-loafing activities was achieved by employing the five-factor model of personality and the theory of interpersonal behaviour (TIB). Several studies have connected cyber-loafing activities with these theories (J-Ho and Ramayah 2017: 75; Sage 2015: 78; Lee and Ohtake 2018: 28).

According to Elciyar and Simsek (2021: 17), cyber-loafing is categorised into minor and serious cyber-loafing based on the severity of the defiant behaviour. Jandaghi *et al.* (2015: 25); Elciyar and Simsek (2021: 56) point out that non-severe or minor cyber-loafing activities include sending and receiving personal emails and reading news using company resources during working hours. Accessing adult websites, logging on to social media, internet banking, online shopping and gambling are some of the cyber-loafing activities that are considered extreme or severe (Jandaghi *et al.* 2015: 25) and Elciyar and Simsek (2021: 56).

Tools that are commonly used by managers as control measures against cyber-loafing were discussed in the literature review section. These tools were identified and explained using the general deterrence theory (GDT), which was adopted by the majority of studies that investigated a similar phenomenon. Other deterrent mechanisms were also used in other instances and these include organisational control mechanisms.

Organisational control was found by Abbasi (2018: 105); Piscotty *et al*. (2016: 66) to be closely associated with managerial control, system control, policy control and behaviour control. Furthermore, the study identified factors influencing the successful implementation of cyber-loafing management tools as follows: workload, working conditions, organisational factors, policies, habits and beliefs, as well as virtual working.

The literature review that steered the empirical study and the summary of key findings are discussed in section 5.3.

5.3 ACHIEVEMENT OF OBJECTIVES

The section presents a summary of the findings gathered from the study. The findings are presented as per the objectives mentioned above.

5.3.1 Objective 1: To identify cyber-loafing activities that are common among administrative staff at eThekwini Municipality Sizakala Customer

Objective 1 was developed to examine and identify cyber-loafing activities that administrative staff engaged in, using the case of eThekwini Municipality Sizakala Customer Care. The results in Chapter Four demonstrate that they were major and minor cyber-loafing activities amongst the investigated administrative staff. These cyber-loafing activities are summarised in Figure 4.15 in the previous chapter. The aforementioned figure indicated that personal emails were ranked highest amongst cyber-loafing deeds.

Activities included by visiting holiday and travel sites, visiting social media sites, pursuing studies, accessing online news, accessing auction sites and checking weather forecasts. Other top activities were ranked between 70 and 81%. The least popular activities were accessing online magazines, gaming and sports and online shopping. All these are social and personal sites that, if misused, do not add value to the work of administrative staff. In line with the above findings, cyber-loafing is divided into two components, which are browsing and emails (Cook 2017: 55).

Browsing actions involve visiting websites for entertainment, financial services, news, social networking, shopping, sports and pornography. To support the preceding result, Aku (2017: 69) stated that e-mailing is another sort of cyber-loafing behaviour that entails receiving and sending e-mails for personal purposes via a company computer and the Internet.

5.3.2 Objective 2: To determine tools used by management to control cyber-loafing by administrative staff at eThekwini Municipality Sizakala Customer Care.

- ***Results based on questionnaires***

The primary finding of the study was that administrative staff revealed that management used some type of tool to control cyber-loafing activities. Based on the results in Chapter Four, 49% of the participants agreed that managers and supervisors monitor workers' internet usage during work hours. As confirmed by 68.3 percent of the participants, monitoring software was used by the organisation to retrieve browsing histories.

Furthermore, the results show that the organisation has an internet use policy that instructs employees on how to use the company internet to avoid cyber-loafing activities. Furthermore, the findings confirmed that managers or supervisors enforced the implementation of the organisation's internet usage policy, which is related to Chapter 2. Control mechanisms were discovered to be in place, including monitoring employee activities during working hours, monitoring software, blocking specific websites, enforcing the Internet usage policy, disciplinary action and continuous awareness of the implications of cyber-loafing activities (Radebe 2020: 46).

According to 60.4% of the respondents, the organisation blocked some sites, making it difficult for employees to access them during working hours. Furthermore, employees who were caught using the company and the Internet for personal purposes faced disciplinary action and regular communications were made about the consequences of engaging in cyber-loafing activities.

- **Results based on Interviews**

According to the study's findings, managers and supervisors have strategies in place to combat cyber-loafing among administrative staff. Managers and

supervisors keep an eye on their employees and walk around them while they work. As a result, they have an Information Technology Department that is responsible for controlling and blocking websites and monitoring computer usage. This relates to Chapter 2, where monitoring discourages non-work-related internet use in particular (Gorenc *et al.* 2016: 16). Monitoring software keeps track of how much time employees spend on corporate computers engaging in non-work-related activities (Arciniega et al. 2017: 36). The application saves browser history, keystrokes and websites visited (Gorenc *et al*. 2016: 26). Unauthorised internet activity can be monitored by recording keystrokes.

The eThekwini Municipality Sizakala Customer Service has an internet usage policy that helps to inform their employees about the consequences of breaking it. According to the literature, well-written policies will encourage positive usage while discouraging activities like cyber-loafing (Kim 2018: 55). Policies promote the flow of information and boost output (Galli 2015: 06). Users will be able to understand and work within the policies' parameters. According to the findings of Chapter 2, Abbasi (2018: 105) discovered that managers use software packages to control and monitor cyber-loafing activities, but managers were not involved in the study. Only the Information Technology Department is in charge of such matters. According to Song (2021:20), organisations primarily used the GDT as control mechanisms and strategies for preventing and mitigating employee cyber-loafing. This contradicts the result of the study; not a single participant from management or administrative staff witnessed staff being charged with violating internet policy. Hence, cyber-loafing takes place within the organisation.

5.3.3 Objective 3: to examine factors affecting the implementation of tools that can be used by management to control cyber-loafing by administrative staff in eThekwini Municipality Sizakala Customer Care

The primary findings revealed that management communication, daily workload, a stressful work environment and organisational culture all had an impact on the implementation of tools that management could use to control cyber-loafing

activities. Based on the study's results, the daily workload was not viewed as a deterrent to cyber-loafing activities. Internet usage monitoring systems did not appear to have an impact on the implementation of control systems for preventing cyber-loafing.

The study also concluded that the workplace environment was stressful to the point where it hampered the implementation of tools for controlling cyber-loafing activities. Furthermore, organisational factors were found to influence the implementation of cyber-loafing tools. This is consistent with the literature. According to research, norms that encourage cyber-loafing among co-workers and supervisors are positively associated with it. This demonstrates the possibility of normative control over cyber-loafing (Jafarkarimi *et al*. 2016: 45). Employees should look to their co-workers as potential workplace role models because (Radebe 2020: 47) cyber-loafing is learned by imitating the behaviours of others in their corporate context (Khansa 2017: 54).

Organisational culture affects the implementation of tools that management could use to control cyber-loafing activities.

5.4 IMPLICATION OF THE STUDY

The roles of managers and supervisors in reducing cyber-loafing are unclear. There was little emphasis placed on evaluating the tools used by managers to control cyber-loafing by administrative staff. As a result, the findings of this study shed light on the role that managers and supervisors can play in reducing cyber-loafing. This work will assist management to identify cyber-loafing activities.

The findings of this study show that some tools used by managers were put in place many years ago, before COVID-19. As technology advances, the world we live in is shifting toward virtual work. This researcher will assist management in reviewing tools, identifying new ones, removing those that are no longer effective and combining those tools with their role in reducing cyber-loafing. Also,

management will be able to identify factors affecting the implementation of tools to control cyber-loafing.

The study will aid company production by employing appropriate tools to control cyber-loafing and involving management in the process. As a result, the productivity and stability of the company will improve. There are policies in place as a result of the study, but in the future, management must collaborate with the information technology department.

This work will also educate administrative staff on the negative effects of cyber-loafing on company growth and how to reduce risk in their organisations by prohibiting harmful internet practices such as visiting websites that contain viruses or inappropriate materials that customers may see. This research adds value to the organisation's economy because cyber-loafing harms company growth.

The theory of interpersonal behaviour aided the researcher in connecting cyber-loafing to the theory's components. However, to explain the increase in technology and its components, the theory must be revisited. The study relies heavily on GDT in identifying tools to control cyber-loafing. However, for the theory to remain relevant, some tools must be reviewed.

5.5. LIMITATIONS OF THE STUDY

The research was carried out at eThekwini Municipality Sizakala Customer Care and the findings are based on a single department of eThekwini Municipality in Durban. Because cyber-loafing is a global problem, other departments and areas may be able to provide more information. As a result, it is suggested that the generalisation of the result be done with caution.

5.6 RECOMMENDATIONS FOR MANAGEMENT

Based on this study's results, the following recommendations can assist the eThekwini Municipality Sizakala Customer Care in managing or preventing cyber-loafing activities.

- Cyber-loafing increases the risk of businesses being exposed to cyber-security, which might be costly in the long run. The company needs to invest in more advanced technology like CCTV cameras to improve its monitoring systems.
- Management's communication with its employees is not effective enough. Management needs to continuously communicate to employees the consequences of cyber-loafing through meetings, emails and memos. Policies should be communicated regularly.
- The induction of new employees is also key to preventing cyber-loafing activities. Employees need to be formally inducted, which can mould their behavioural intentions towards deviant behaviours at work.
- Continuous enforcement of the disciplinary code of conduct is needed. If employees see others being disciplined for unwanted behaviour, they will take the rules and policies seriously, knowing the consequences.
- There is a need for the organisation to incorporate trust in their employees as a strategy to prevent cyber-loafing.

5.7 RECOMMENDATIONS FOR FUTURE STUDIES

- There is a need for a comparative analysis of private, parastatals and government institutions on mechanisms used to control cyber-loafing activities.
- This study did not investigate staff performance in cyber-loafing activities. Further studies are recommended to investigate how cyber-loafing activities affect employee performance.

- The study was based on a customer care setup where employees deal customer complaints issues. Thus, more studies should look into other areas unrelated to customer care.

5.8 CONCLUSION

Cyber-loafing has become a standard practice being carried out by employees in many organisations. This study corroborates the existing literature that cyber-loafing activities are common in the workplace, including administrative staff at eThekwini Municipality Sizakala Customer Care. Despite the existence of mitigating mechanisms implemented by management at the investigated site, cyber-loafing is still prevalent. This is a clear indication that the implementation of these tools falls short. This research concluded that there are factors affecting the successful implementation of tools that are used by management to control cyber-loafing. These factors included communication from management, daily workload, a stressful office environment and organisational culture.

REFERENCES

Aaij, R., Beteta, C.A., Adeva, B., Adinolfi, M., Aidala, C.A., Ajaltouni, Z., Akar, S., Albicocco, P., Albrecht, J., Alessio, F. and Alexander, M., 2019. Measurement of charged hadron production in Z-tagged jets in proton-proton collisions at s= 8 TeV. *Physical Review Letters*, *123*(23), p.232001.

Abbasi, H.A. 2018. *Organizational information security: Strategies to minimize workplace cyberloafing for increased productivity* Doctor of Philosophy Walden University

Abubakar, A.M. and Al-zyoud, M.F., 2021. Problematic Internet usage and safety behavior: Does time autonomy matter?. *Telematics and Informatics*, *56*, p.101501.

Ali, M., Kwon, Y.S., Lee, C.H., Kim, J. and Kim, Y. eds., 2015. Current Approaches in Applied Artificial Intelligence: 28th International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, IEA/AIE 2015, Seoul, South Korea, June 10-12, 2015, Proceedings.

Aku, A. 2017. *Role of middle managers in mitigating employee cyberloafing in the workplace*. Doctor of Philosophy Dissertation Walden University. Available at:https://www.researchgate.net/deref/https%3A%2F%2Fscholarworks.waldenu.edu%2Fdissertations%2F3967.

AKBULUT, A., 2017. Implementation of zigbee (ieee 802.15. 4) based wireless ecg measurement system. *International Journal of Engineering Research and Development*, *9*(3), pp.43-53.

Albers, M.J. 2017. *Introduction to Quantitative Data Analysis in the Behavioral and Social Sciences*. [online] John Wiley & Sons. Available at: https://www.wiley.com/en-

us/Introduction+to+Quantitative+Data+Analysis+in+the+Behavioral+and+Social+Sciences-p-9781119290186 [Accessed 28 Nov. 2022].

Andel, S.A., Kessler, S.R., Pindek, S., Kleinman, G. and Spector, P.E. 2019. Is cyberloafing more complex than we originally thought? Cyberloafing as a coping response to workplace aggression exposure. *Computers in Human Behavior*, *101*, pp.124-130.

Andreassen, C.S., Torsheim, T. and Pallesen, S. 2014. Predictors of use of social network sites at work-a specific type of cyberloafing. *Journal of Computer-Mediated Communication*, *19*(4), pp.906-921.

Askew, K., Buckner, J.E., Taing, M.U., Ilie, A., Bauer, J.A. and Coovert, M.D. 2014. Explaining cyberloafing: The role of the theory of planned behavior. *Computers in Human Behavior, [online] 36, pp.510–519. doi:10.1016/j.chb.2014.04.006.*

Arciniega, H., Kilgore-Gomez, A., Harris, A., Peterson, D.J., McBride, J., Fox, E. and Berryhill, M.E., 2019. Visual working memory deficits in undergraduates with a history of mild traumatic brain injury. *Attention, Perception, & Psychophysics*, *81*(8), pp.2597-2603.

Bhagat, P. and Shimray, S.R., 2021. Smartphone Usage among University Students during the Covid-19 pandemic: A Study. *Library Philosophy and Practice*, pp.1-10.

Barlow, D.H., Ellard, K.K., Sauer-Zavala, S., Bullis, J.R. and Carl, J.R., 2014. The origins of neuroticism. *Perspectives on Psychological Science*, *9*(5), pp.481-496.

Baturay, M.H. and Toker, S., 2015. An investigation of the impact of demographics on cyberloafing from an educational setting angle. *Computers in Human Behavior*, *50*, pp.358-366.

Bhattacherjee, A. 2012. *Social science research: Principles, methods and practices*. Textbooks Collection. 3. http://scholarcommons.usf.edu/oa_textbooks

Blau, G., Yang, Y. and Ward-Cook, K. 2006. Testing a measure of cyberloafing. *Journal of allied health*, *35*(1), pp.9-17.

Bullen, P.B. 2014. How to pretest and pilot a survey questionnaire. *Retrieved from*.http://www.tools4dev.org/resources/how-to-pretest-and-pilot-a-survey-questionnaire/ [Accessed November 8 2019]

Byrne, D., 2022. A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & quantity*, *56*(3), pp.1391-1412.

Chang, M.K. and Cheung, W. 2001. Determinants of the intention to use Internet/WWW at work: a confirmatory study. *Information & Management*, *39*(1), pp.1-14.

Chen, Q., Gong, Y., Lu, Y. and Chau, P.Y. 2022. How mindfulness decreases cyberloafing at work: a dual-system theory perspective. *European Journal of Information Systems*, pp.1-17.https://doi.org/10.1080/0960085X.2022.2067490

Chen, Y., Chen, H., Andrasik, F. and Gu, C. 2021. Perceived stress and cyberloafing among college students: The mediating roles of fatigue and negative coping styles. *Sustainability*, *13*(8), p.4468.

Cheng, L., Li, W., Zhai, Q. and Smyth, R. 2014. Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, *38*, pp.220-228.

Coti, I., Haberl, T., Scherzer, S., Werner, P., Shabanian, S., Kocher, A., Laufer, G. and Andreas, M., 2020. Outcome of rapid deployment aortic valves: long-term experience after 700 implants. *Annals of cardiothoracic surgery*, *9*(4), p.314.

Corbett, K.S., Flynn, B., Foulds, K.E., Francica, J.R., Boyoglu-Barnum, S., Werner, A.P., Flach, B., O'Connell, S., Bock, K.W., Minai, M. and Nagata, B.M., 2020. Evaluation of the mRNA-1273 vaccine against SARS-CoV-2 in nonhuman primates. *New England Journal of Medicine*, *383*(16), pp.1544-1555.

Cope, D.G., 1969. Methods and meanings: Credibility and trustworthiness of qualitative research. *Number 1/January 2014*, *41*(1), pp.89-91.

Creswell, J.D., 2017. Mindfulness interventions. *Annual review of psychology*, *68*(1), pp.491-516.

Dalgıç, B., Fazlıoğlu, B. and Karaoğlan, D., 2015. Entry to foreign markets and productivity: Evidence from a matched sample of Turkish manufacturing firms. *The Journal of International Trade & Economic Development*, *24*(5), pp.638-659.

Dar, A.A., Parihar, P.S., Saleh, P. and Malik, M.A., 2018. Variable stars in M37. *Research in Astronomy and Astrophysics*, *18*(12), p.155.

Demarchi, L.O., Scudeller, V.V., Moura, L.C., Lopes, A. and Piedade, M.T.F., 2019. Logging impact on Amazonian white-sand forests: perspectives from a sustainable development reserve. *Acta Amazonica*, *49*, pp.316-323.

Del Sole, F., Farcomeni, A., Loffredo, L., Carnevale, R., Menichelli, D., Vicario, T., Pignatelli, P. and Pastori, D., 2020. Features of severe COVID-19: a systematic review and meta-analysis. *European journal of clinical investigation*, *50*(10), p.e13378.

Dmour, M.M., Bakar, H.S. and Hamzah, M.R. 2020, April. Antecedent, Consequences and Policies View of Cyberloafing among the Employees. In *Journal of Physics: Conference Series* (Vol. 1529, No. 2, p. 022016). IOP Publishing.

Dudovskiy, J., 2016. Research Methodolgy. *J. Dudovskiy, The Ultimate Guide to Writing a Dissertation in Business Studies: A step-by-step Assistance. Retrieved*, *10*(29), p.2016.

Dooly, V.P., 2021. *Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study* (Doctoral dissertation, Walden University).

Elciyar, K. and Simsek, A. 2021. An investigation of cyberloafing in a large-scale technology organization from the perspective of the theory of interpersonal behavior. *Online Journal of Communication and Media Technologies*, *11*(2), p.e202106. https://doi.org/10.30935/ojcmt/10823

Erlandson, D.A., Harris, E.L., Skipper, B.L. and Allen, S.D., 1993. *Doing naturalistic inquiry: A guide to methods*. Sage.

Ezeh, L.N., Etodike, C.E. and Chukwura, E.N. 2018. Abusive supervision and organizational cynicism as predictors of cyber-loafing among federal civil service employees in Anambra State, Nigeria. *European Journal of Human Resource Management Studies*. Vol 1, No 2 http://dx.doi.org/10.46827/ejhrms.v0i0.319

Faezi, N.A., Gholizadeh, P., Sanogo, M., Oumarou, A., Mohamed, M.N., Cissoko, Y., Sow, M.S., Keita, B.S., Baye, Y.A.M., Pagliano, P. and Akouda, P., 2021. Peoples' attitude toward COVID-19 vaccine, acceptance, and social trust among African and Middle East countries. *Health Promotion Perspectives*, *11*(2), p.171.

Galluch, P.S., Grover, V. and Thatcher, J.B., 2015. Interrupting the workplace: Examining stressors in an information technology context. *Journal of the Association for Information Systems*, *16*(1), p.2.

Garrett, R.K. and Danziger, J.N. 2008. Disaffection or expected outcomes: Understanding personal Internet use during work. *Journal of Computer-Mediated Communication*, *13*(4), pp.937-958.

Glassman, J., Prosch, M. and Shao, B.B. 2015. To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management*, *52*(2), pp.170-182.

Gorenc, M. and Braz, M., 2020. Factors affecting a successful coordination of sports and academic careers. *Management*, *20*, p.22.

Grimm, P. 2010. Pretesting a questionnaire. *Wiley International Encyclopaedia of Marketing*.

Hadlington, L. and Parsons, K. 2017. Can cyberloafing and Internet addiction affect organizational information security? *Cyberpsychology, Behavior and Social Networking*, *20*(9), pp.567-571.

Hartijasti, Y. and Fathonah, N., 2014. Cyberloafing across Generation X and Y in Indonesia. *Journal of Information Technology Applications and Management*, *21*(1), pp.1-16

Hassan, S., Nadzim, S.Z.A. and Shiratuddin, N., 2015. Strategic use of social media for small business based on the AIDA model. *Procedia-Social and Behavioral Sciences*, *172*, pp.262-269.

Hagqvist, E., Vinberg, S., Tritter, J.Q., Wall, E. and Landstad, B.J., 2020. The same, only different: doing management in the intersection between work and private life for men and women in small-scale enterprises. *Work, Employment and Society*, *34*(2), pp.262-280.

Hassan, H.M., Reza, D.M. and Farkhad, M.A.A., 2015. An experimental study of influential elements on cyberloafing from general deterrence theory perspective: Case study: Tehran subway organization. *International Business Research*, *8*(3), p.91.

Hensel, P.G. and Kacprzak, A. 2021. Curbing cyberloafing: studying general and specific deterrence effects with field evidence. *European Journal of Information Systems*, *30*(2), pp.219-235.

Holguin, E.S. 2016. *Strategies functional managers use to control cyberloafing behaviors* (Doctoral dissertation, Walden University).

Huang, J.L., Liu, M. and Bowling, N.A., 2015. Insufficient effort responding: examining an insidious confound in survey data. *Journal of Applied Psychology*, *100*(3), p.828.

Ince, M. and Gül, H, 2011. The role of the organizational communication on employees' perception of justice: A sample of public institution from Turkey.

Issock, P.B.I., Roberts-Lombard, M. and Mpinganjira, M., 2020. Normative influence on household waste separation: the moderating effect of policy implementation and sociodemographic variables. *Social Marketing Quarterly*, *26*(2), pp.93-110.

Jandaghi, G., Alvani, S.M., Zarei Matin, H. and Fakheri Kozekanan, S. 2015. Cyberloafing management in organizations. *Iranian Journal of Management Studies*, *8*(3), pp.335-349.

Jafarkarimi, H., Sim, A.T.H., Saadatdoost, R. and Hee, J.M., 2016. Facebook addiction among Malaysian students. *International Journal of Information and Education Technology*, *6*(6), p.465.

Kanholkar, K. and Dharkar, N. 2022. *Research Methodology*. Ashok Yakkaldevi.

Kasap, Y. 2019. *Cyberloafing behavior in the workplaces and management practices* (Doctoral dissertation, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü).

Kumar, M.D. and Govindarajo, N.S., 2014. Instrument Development:“Intention to Leave Instrument”(ILI). *Middle-East Journal of Scientific Research*, *21*(3), pp.509-517.

Kothari, C.R. 2004. *Research methodology: Methods and techniques*. New Age International.

Krzych, Ł., Lach, M., Joniec, M., Cisowski, M. and Bochenek, A. 2018. The Likert scale is a powerful tool for quality-of-life assessment among patients after minimally invasive coronary surgery. *Kardiochirurgia i Torakochirurgia Polska/Polish Journal of Thoracic and Cardiovascular Surgery*, *15*(2), pp.130-134.

Kaptangil, İ., 2021. Covid-19 pandemic: reflections on organizational life and employee psychology. In *Contemporary Issues in Social Science* (Vol. 106, pp. 221-238). Emerald Publishing Limited.

Koay, K.Y. and Poon, W.C., 2022. Understanding Students' Cyberslacking Behaviour in e-Learning Environments: Is Student Engagement the Key?. *International Journal of Human–Computer Interaction*, pp.1-16.

Kumar, R. 2018. *Research methodology: A step-by-step guide for beginners*. Sage.

Kumar, D. 2016. *Building sustainable competitive advantage: Through executive enterprise leadership*. Routledge.

Ozdamli, F. and Cavus, N., 2021. Knowledge sharing technologies in higher education: Preferences of CIS students in Cyprus. *Education and Information Technologies*, *26*(2), pp.1833-1846.

Lettieri, C., Zavalloni, D., Rossini, R., Morici, N., Ettori, F., Leonzi, O., Latib, A., Ferlini, M., Trabattoni, D., Colombo, P. and Galli, M., 2015. Management and

long-term prognosis of spontaneous coronary artery dissection. *The American journal of cardiology*, *116*(1), pp.66-73.

Lim, T.L.W., Tan, K.H., Tee, C.S. and Yeo, G.S.H., 2005. Investigating stillbirths using a simplified obstetric events-based protocol. *Singapore medical journal*, *46*(2), p.63.

Lobe, B., Morgan, D. and Hoffman, K.A. 2020. Qualitative data collection in an era of social distancing. *International journal of qualitative methods*, *19*, p.1609406920937875.

Marcolino, M.S., Ziegelmann, P.K., Souza-Silva, M.V., Nascimento, I.J.B.D., Oliveira, L.M., Monteiro, L.S., Sales, T.L., Ruschel, K.B., Martins, K.P., Etges, A.P.B. and Molina, I., 2021. Clinical characteristics and outcomes of patients hospitalized with COVID-19 in Brazil: Results from the Brazilian COVID-19 registry. *International Journal of infectious diseases*, *107*, pp.300-310.

Mackey, A. and Gass, S.M. 2015. *Second language research: Methodology and design*. Routledge.

Malik, J., Rodriguez, J., Weisbloom, M. and Petridis, H., 2018. Comparison of accuracy between a conventional and two digital intraoral impression techniques. *International Journal of Prosthodontics*, *31*(3), pp.107-113.

McCreary, D.R., Fong, I. and Groll, D.L., 2017. Measuring policing stress meaningfully: establishing norms and cut-off values for the Operational and Organizational Police Stress Questionnaires. *Police Practice and Research*, *18*(6), pp.612-623.

Messner, N., Woods, A., Petty, A., Parmar, P.K., Leigh, J., Thomas, E., Curry, D., Venters, H., Gilbert, A., Nelson, T. and Lester, E., 2019. Qualitative evidence of crimes against humanity: the August 2017 attacks on the Rohingya in northern Rakhine State, Myanmar. *Conflict and health*, *13*(1), pp.1-17.

Miyara, M., Chader, D., Sage, E., Sugiyama, D., Nishikawa, H., Bouvry, D., Claër, L., Hingorani, R., Balderas, R., Rohrer, J. and Warner, N., 2015. Sialyl Lewis x (CD15s) identifies highly differentiated and most suppressive FOXP3high regulatory T cells in humans. *Proceedings of the National Academy of Sciences*,*112*(23), pp.7225-7230

Mohajan, H.K. 2018. Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), pp.23-48.

Mohammed, A., Sheikh, T.L., Gidado, S., Poggensee, G., Nguku, P., Olayinka, A., Ohuabunwo, C., Waziri, N., Shuaib, F., Adeyemi, J. and Uzoma, O., 2015. An evaluation of psychological distress and social support of survivors and contacts of Ebola virus disease infection and their relatives in Lagos, Nigeria: a cross sectional study− 2014. *BMC Public Health*, *15*(1), pp.1-8.

Nandi, A. and Platt, L. 2017. Are there differences in responses to social identity questions in face-to-face versus telephone interviews? Results of an experiment on a longitudinal survey. *International Journal of Social Research Methodology*, *20*(2), pp.151-166.

Nayak, J.K. and Singh, P., 2021. *Fundamentals of research methodology problems and prospects*. SSDN Publishers & Distributors.

Nguyen, T.T.M. 2019. Data collection methods in L2 pragmatics research: An overview. *The Routledge handbook of second language acquisition and pragmatics*, pp.195-211.

Patton, M.Q., 1990. *Qualitative evaluation and research methods*. SAGE Publications, inc.

Pandey, P. and Pandey, M.M. 2021. *Research methodology tools and techniques*. Bridge Center.

Polit, D.F. and Beck, C.T., 2013. Is there still gender bias in nursing research? An update. *Research in nursing & health*, *36*(1), pp.75-83.

Piscotty, R., Martindell, E. and Karim, M. 2016. Nurses' self-reported use of social media and mobile devices in the work setting. *On-Line Journal of Nursing Informatics*, *20*(1).

Radebe, T.G., 2020. *Psychological well-being and coping in the context of employee stress* (Doctoral dissertation, North-West University (South Africa).

Ramalingam, K. and Jiar, Y.K. 2022. The Recent Trends on The Speaking Skills with Storytelling Approach. *International journal of special education*, *37*(3s).

Reo, Y.J., Jun, Y.W., Cho, S.W., Jeon, J., Roh, H., Singha, S., Dai, M., Sarkar, S., Kim, H.R., Kim, S. and Jin, Y., 2020. A systematic study on the discrepancy of fluorescence properties between in solutions and in cells: super-bright, environment-insensitive benzocoumarin dyes. *Chemical Communications*, *56*(72), pp.10556-10559.

Quan-Haase, A. and Sloan, L. eds., 2022. *The SAGE handbook of social media research methods*. Sage.

Ohtake, P.J., Lee, A.C., Scott, J.C., Hinman, R.S., Ali, N.A., Hinkson, C.R., Needham, D.M., Shutter, L., Smith-Gabai, H., Spires, M.C. and Thiele, A., 2018. Physical impairments associated with post–intensive care syndrome: systematic review based on the world health organization's international classification of functioning, disability and health framework. *Physical therapy*, *98*(8), pp.631-645.

Örün, Ö. and Akbulut, Y., 2019. Effect of multitasking, physical environment and electroencephalography use on cognitive load and retention. *Computers in Human Behavior*, *92*, pp.216-229.

Sampat, B. and Basu, P.A., 2017. Cyberloafing: The Di (sguised) gital Way of Loafing on the Job. *IUP Journal of Organizational Behavior*, *16*(1).

Schoonenboom, J. and Johnson, R.B. 2017. How to construct a mixed methods research design. *Kölner Zeitschrift für Soziologie und Sozialpsychologie*, *69*(2), pp.107-131.

Şimşek, A. and Şimşek, E. 2019. Beneficial and detrimental effects of cyberloafing in the workplace. *Journal of Organizational Behavior Review*, *1*(1), pp.97-114.

Singh, K.K. 2022. *Research Methodology in Social Science*. KK Publications.

Taherdoost, H. 2016. Validity and reliability of the research instrument; how to test the validation of a questionnaire/survey in research. *How to test the validation of a questionnaire/survey in research (August 10, 2016)*.

Tandon, A., Kaur, P., Ruparel, N., Islam, J.U. and Dhir, A., 2021. Cyberloafing and cyberslacking in the workplace: systematic literature review of past achievements and future promises. *Internet Research*.

Toker, S. and Baturay, M.H., 2021. Factors affecting cyberloafing in computer laboratory teaching settings. *International Journal of Educational Technology in Higher Education*, *18*(1), pp.1-24.

Thompson, J., 2022. A guide to abductive thematic analysis. *The Qualitative Report*, *27*(5), pp.1410-1421.

Willis, G.B. 2004. *Cognitive interviewing: A tool for improving questionnaire design*. sage publications.

ŞİMŞEK, A. and ŞİMŞEK, E., 2019. Beneficial and detrimental effects of cyberloafing in the workplace. *Journal of Organizational Behavior Review*, *1*(1), pp.97-114.

Song, M., Ugrin, J., Li, M., Wu, J., Guo, S. and Zhang, W., 2021. Do deterrence mechanisms reduce cyberloafing when it is an observed workplace norm? A

moderated mediation model. *International Journal of Environmental Research and Public Health*, *18*(13), p.6751.

Ugrin, J.C. and Pearson, J.M., 2013. The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, *29*(3), pp.812-820.

Yin, C. 2003. Research Methodology: Methods & Techniques. *New age International Publishers, New Delhi, India*.

Zaka, A., Akhter, A.S., Jabeen, R. and Sanaullah, A., 2021. Control charts for the shape parameter of reflected power function distribution under classical estimators. *Quality and Reliability Engineering International*, *37*(6), pp.2458-2477.

Zhang, J., Meng, M., Wong, Y.D., Ieromonachou, P. and Wang, D.Z., 2021. A data-driven dynamic repositioning model in bicycle-sharing systems. *International Journal of Production Economics*, *231*, p.107909

Zohurian, M. and Rahimnia, F., 2015. Designing a model for sustainable Development of business Clusters in iran. *Journal of Entrepreneurship Development*, *8*(1), pp.41-59.

Zu, Z.Y., Jiang, M.D., Xu, P.P., Chen, W., Ni, Q.Q., Lu, G.M. and Zhang, L.J., 2020. Coronavirus disease 2019 (COVID-19): a perspective from China. *Radiology*, *296*(2), pp.E15-E25.

APPENDICES

APPENDIX A: LETTER OF INFORMATION

Title of the Research Study: Evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff.

Principal Investigator/s/researcher: Nonhlanhla Beata Mkhize

Co-Investigator/s/supervisor/s: Dr. CJ Nyide and Dr. Mthalane

Brief Introduction and Purpose of the Study: The use of the Internet has improved productivity and communication in the workplace. However, employees tend to abuse this innovation by engaging in cyber-loafing practices. When cyber-loafing, employees use their employers' time and computers for their personal use. This has created a huge problem for organizations in controlling such behaviour, which has resulted in employees being unproductive. Research has shown that managers lack the correct skills and strategies for mitigating cyber-loafing practised by employees in the workplace. Organizations are losing out due to cyber-loafing (Gholamera Jandaghi, 2015) which include identity theft, time wasted, personal usage of internet by employees and lack of innovation which result from divided attention of employees engaging in cyber-loafing. Some of these events are not formally dealt with because of the cost that engaging in dealing or resolving this act by employees. Nowadays, most organization are adopting formal methods of checking the usage of the Internet and computers to deal with cyber-loafing phenomenon. Although companies have discovered many tools to control cyber-loafing behaviour that is employed by managers to control cyber-loafing activities, hence the number of employees that embark in cyber-loafing still accumulate so they are a need

to evaluate or to test the effectiveness of the existing cyber-loafing tools or suggest the new ones. The aim of conducting this study is to evaluate control mechanisms and the role that managers can play in mitigating cyber-loafing in their workplaces. A mixed method as suggested by (Creswell 2015: 5) which involves using multiple sources of data or multiple approaches to analysing data to enhance the credibility of the research study. Data originating from navigational and surveying contexts and through triangulation aligns multiple perspectives will lead to a more comprehensive analysis. This study will be conducted at the eThekwini Municipality Sizakala Customer Care.

Greetings. Greetings all

Introduce yourself to the participant: I am a student at DUT doing research in

Master of Management Sciences in Administration and Information Management.

Invitation to the potential participant: I would like to invite you to take part in the research.

What is Research: Research is a systematic search or enquiry for generalised new knowledge.

The language that is going to be used by the researcher is free of jargon and unexplained acronyms and it will be easily understood by the potential research participant. Technical terminology, which will be included will be clear and explained. Consider the age, target population, home language, educational level, frame of mind, etc. of the participant. An explanation to the potential participant that he/she can ask as many questions as he/she wish because it is important that he/she fully understand the study. Participants are entitled to discuss the study with their family and friends and are under no obligation to commit at this stage. For this purpose, a copy of the Letter of Information document is given to the potential participant to take home.)

Outline of the Procedures: All participants of the study will be treated with respect and any information given will be solely for the study. The researcher will apply for an

ethical clearance through the research office. The questionnaire will take 15 minutes of the participant's time to complete and participation is voluntary. The participant can withdraw from the study anytime without giving reasons. The information the respondent gives will only be used for research purposes.

Data collection involves applying the measuring instrument to the sample selected for the investigation (Dudovskiy 2018: 5). Mixed methods data collection is so much useful in comprehending contradictions between qualitative and quantitative result and qualitative findings. Mixed method data collection will also ensure that it give voice to the study participants and ensure that the study findings are rooted in the participant's experiences. For the researcher to accomplish the purpose of the study qualitative and quantitative data collection will be employed.

Risks or Discomforts to the Participant: Minimal risk as human are involved

Explain to the participant the reasons he/she may be withdraw from the Study: The research may be terminated early in particular circumstances viz. Non-compliance, illness, adverse reactions, etc. State that the participant is entitled to withdraw from the study at any time should they wish to do so and will still continue to receive the appropriate standard of care; The potential participant that the research may be terminated early in particular circumstances. The researcher may, under certain circumstances, decide to withdraw the participant from the study;

A participant can leave a research study at any time. When withdrawing from the study, the participant should let the research team know that he/she wishes to withdraw. A participant may provide the research team with the reason(s) for leaving the study but is not required to provide their reason.

Depending on the type of study, the participant may be given a variety of instructions for ending his/her participation in the study. For instance, a participant may be given instructions on how to safely stop using study medications. Instructions may also be given on who to contact if there are any questions or concerns that arise after

completing the study. The research team may need to have the participant return so that he/she can be monitored for any future adverse effects from the study treatments, procedures, or interventions.

If the study involves collection of health information, at the time of withdrawal, the research participant should let the research team know if he/she will allow the continued collection and use of his/her health information by the researchers.

Non-compliance? Of the participant? Standard of care?

The Institution Research Ethics Committee (IREC) has the responsibility of evaluating, approving and monitoring research involving humans, animals and the environment. It does so by following accepted research ethical guidelines as laid out by the Department of Health of South Africa and the Declaration of Helsinki. It aims to protect the rights and welfare of research participants, animals and the environment by adhering to the principles of beneficence, justice and respect for persons, especially vulnerable populations, animals and the environment. In so doing it must ensure that the research methodology and relevant literature is based on sound principles derived from appropriate studies with the aim to provide an answer to the research question posed.

The committee membership is composed as required by the National Health Research Council of South Africa, which is the accrediting body. All members are required to have initial and ongoing training in Research ethics.

Benefits: A journal article will be written for an accredited academic journal in the field of Accounting and Informatics.

Remuneration: There will be no remuneration received by the participant.

Costs of the Study: There will be no costs of the study expected from participant towards the completion of the study.

Confidentiality: All participants of the study will be treated with respect and any

information provided by participant personal or professional, will be confidential. The researcher will apply for an ethical clearance through the research office. The study will not affect participants personally or professionally. Researchers are entitled to keep data sets confidential before publication. b. After publication, when the research is in the public domain, the data should, upon request, be available to other researchers by the Principal Investigator. Despite any technical or cost problems that may prevent it being made available the principle is that there should be an opportunity for checking any data on which material in the public domain is based. c. Confidentiality of data collected during any research project is essential. All personal information should be encoded or anonymised as much as possible and be consistent with the needs of the study. Participants should be assigned a reference number or code as early as possible and data should be stored against this number/code rather than against the names of the participants. Investigators may wish to maintain separate lists of people who have taken part in their research, but steps should be taken to ensure that it is not possible to relate a particular set of data back to any given participant. The requirement for data availability does not override the right to confidentiality and privacy of individuals or organizations who are subjects of research.

Results: The results from this study will be presented in writing in journals. At no time, however, will your name be used, or any identifying information revealed. If you wish to receive a copy of the results from this study, you may contact the researchers at the telephone number given below.

Research-related Injury: Minimal risk as human are involved

Storage of all electronic and hard copies including tape recordings

Research Data storage and maintenance a. It is the responsibility of the researcher to arrange for safe storage of all data and speciments on which research is based. Costs of such storage should be included in the budgets of research programmes. b. Electronic data sets should have adequate arrangements for back up. Ensuring this is the responsibility of the researcher. c. The primary data should be stored in the

department/programme in which the project is based. The intention of this is to ensure safety and integrity of the data set. The overall responsibility for this rests with the Head of Department/Programme. d. Data on which any publication is based should be retained in the department/programme for at least five years after publication. e. If a researcher leaves the University, the University and the researcher are jointly responsible for ensuring that satisfactory arrangements are made for maintenance of the data set. If there is no contractual arrangement to determine what is to be done with the data, then possible arrangements are: The data set is retained in the University. The researcher has access to the original data set and may keep copies. The data set is transferred to the research institution to which the researcher is moving, provided that adequate facilities are available for conservation and storage. If no publications have appeared on the data set in the last five years, it may be destroyed.

Guidelines for storage of different types of data sets a. Numerical and statistical data Numerical or statistical data should be stored in raw data format for five years from completion of the project. After this time the data should be destroyed unless it is to be used in a longitudinal study's. Interview/Notes/Questionnaire Responses/Transcribed Interviews Wherever possible interview notes/questionnaire responses/transcribed interviews should be stored in their original form for five years from the completion of the project. Unless data is to be used in later longitudinal studies it may be destroyed after this time. Note: Work that informs national policy making should be archived after 10 years. c. Images/Audio and Video Recordings Images/Audio and Video Recordings should be retained in their original form. This is particularly important where they are subsequently enhanced. Wherever possible, both original and enhanced images/audio and video recordings should be kept for five years from completion of the project. Unless data is to be used in longitudinal studies it may be destroyed after this period. d. Blood Samples the University suggests that blood and plasma samples should be anonymised, stored for 3-6 months whilst analysis is conducted, then disposed of in an appropriate manner (in accordance with the code of conduct for people of practice for persons having contact with Human Body Fluids). e. Longitudinal Studies Data gathered as part of a known longitudinal study should be kept for the duration of the study and retained

for ten years after the completion of the study. Participants should be kept informed of how long the study is likely to last. If the study is extended, all participants should be contacted and informed that their data is still being stored and may be used. It is important that participants are given the opportunity to withdraw their data at any point during the study. Note: The importance of maintaining data in its original form is a necessary precaution, particularly if published results are challenged by others.

Persons to contact in the Event of Any Problems or Queries:(Supervisor and details) Please contact the researcher Nonhlanhla 073722561l, my supervisor Dr Nyide 033 845 8804 or the Institutional Research Ethics Administrator on 031 373 2375. Complaints can be reported to the Director: Research and Postgraduate Support Dr. L Linganiso on 031 373 2577 or researchdirector@dut.ac.za.

A copy of the information letter should be issued to participants. The information letter and consent form must be translated and provided in the primary spoken language of the research population e.g., isiZulu.

APPENDIX B: CONSENT

Full Title of the Study: Evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff.

Names of Researcher/s: Nonhlanhla Beata Mkhize

Statement of Agreement to Participate in the Research Study:

☐ I hereby confirm that I have been informed by the researcher, Nonhlanhla Beata Mkhize, about the nature, conduct, benefits and risks of this study

- Research Ethics Clearance Number: _____,

☐ I have also received, read and understood the above written information (Participant Letter of

Information) regarding the study.

☐ I am aware that the results of the study, including personal details regarding my sex, age, date of birth, initials and diagnosis will be anonymously processed into a study report.

☐ In view of the requirements of research, I agree that the data collected during this study can be processed in a computerised system by the researcher.

☐ I may, at any stage, without prejudice, withdraw my consent and participation in the study.

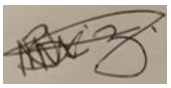
☐ I have had sufficient opportunity to ask questions and (of my own free will) declare myself prepared to participate in the study.

☐ I understand that significant new findings developed during the course of this research which may relate to my participation will be made available to me.

Full Name of Participant	**Date**	**Time**	**Signature/Right Thumbprint**

I, a Beata Mkhize herewith confirm that the above participant has been Nonhlanhl fully
informed about the nature, conduct and risks of the above study.

Nonhlanhla Beata Mkhize 2021/04/15



Full Name of Researcher	**Date**	**Signature**

Full Name of Witness (If applicable)	**Date**	**Signature**

Full Name of Legal Guardian (If applicable)	**Date**	**Signature**

APPENDIX C: DATA COLLECTION TOOLS

QUESTIONNAIRE FOR ADMINISTRATIVE STAFF:

“An evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff: A case of eThekwini Municipality Sizakala Customer Care”.

Researcher: Nonhlanhla Beata Mkhize

Supervisor: Dr. Nyide

Co-Supervisor: Dr. Mthalane

Department of Finance and Information Management

Faculty of Accounting and Informatics

Durban University of Technology

ETHICAL CLEARANCE NO: …….

Please kindly complete this questionnaire.

Please note that there is no correct/incorrect answer.

Please note that participation in the study is voluntary.

Please sign the letter of informed consent, permitting me to use your responses for this research project.

Please kindly take note of the instructions before answering any question(s).

For sections where it stated, mark the applicable block with the correct information (with a cross (X).

1.	Age:	☐ 18 – 30	☐ 31 – 40	☐ 41-50	☐ 51 and above

2.	Gender:	☐ Female	☐ Male

3.	Ethnicity:	☐ African	☐ Indian	☐ Coloured	☐ White
		Others (please specify):			

4.	Academic level:	☐ Grade 11 or less	☐ Matric	☐ Certificate	☐ Diploma
		☐ Degree	Others (please specify):		

Please answer all the questions as this will provide more information for the researcher so that accurate analysis and interpretation of data can be made.

Thank you for your co-operation. The researcher hopes that you will find the questionnaire interesting and stimulating.

SECTION A: DEMOGRAPHIC INFORMATION

The following information is needed to help the researcher with the statistical analysis of data regarding the evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff. All your responses will be treated with confidentiality. The researcher appreciates your help in providing this important information.

SECTION B: CYBER-LOAFING ACTIVITIES THAT ARE COMMON AMONGST ADMINISTRATIVE STAFF:

Place an X mark in the box of your answer.

		Never	Rarely	Sometimes	Often	Always
1.	I use work computers and/ or internet to do online shopping.					
2.	I use work computers and/ or internet for gaming and sports.					
3.	I use work computers and/ or internet to visit holiday and travel sites.					
4.	I use work computers and/ or internet to visit social media sites.					

5.	I use work computers and/ or internet to access job search sites.					
6.	I use work computers and/ or internet to pursue my studies.					
7.	I use work computers and/ or internet to access online news sites.					
8.	I use work computers and/ internet to access online magazines.					
9.	I use work computers/ or internet to access auction sites.					
10.	I use work computers/ or internet to check the weather forecast.					
11.	I use work computers and internet to access my personal emails.					

SECTION C: TOOLS USED BY MANAGERS TO CONTROL CYBER-LOAFING ACTIVITIES BY ADMINISTRATIVE STAFF

Place an X mark in the box of your answer.

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
12.	Managers/ supervisors monitor the Internet usage by workers during work hours.					
13.	Monitoring software is used by the organisation to retrieve browsing history.					
14.	My organisation has the Internet usage policy.					
15.	The internet usage policy that is adequate to limit cyber-loafing activities in my organisation.					
16.	Managers/ supervisors enforce the implementation of the Internet usage policy in my organisation.					

17.	I am unable to access some websites because they are blocked by my organisation.					
18.	Employees who are caught using company computers and the Internet for personal use face disciplinary action.					
19.	Employees are formally informed of the implications of engaging in cyber-loafing.					

SECTION D: FACTORS AFFECTING THE IMPLEMENTATION OF TOOLS THAT CAN BE USED TO CONTROL CYBER-LOAFING ACTIVITIES BY ADMINISTRATIVE STAFF

Place an X mark in the box of your answer.

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
20.	Communication from management on the Internet usage policy is adequate.					

21.	My daily workload prevents me from using the Internet for personal use.					
22.	Internet usage monitoring systems prevent me from using the Internet for personal use.					
23.	The stressful office environment encourages me to engage in cyber-loafing activities.					
24.	The organisation culture encourages me to engage in cyber-loafing.					
25.	Disciplinary actions against employees contravening internet usage policy prevent me from engaging in cyber-loafing activities.					

THANK YOU VERY MUCH FOR YOUR TIME!

INTERVIEW QUESTIONS FOR SUPERVISORS AND MANAGERS

“An evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff: A case of eThekwini Municipality Sizakala Customer Care”.

Researcher: Nonhlanhla Beata Mkhize

Supervisor: Dr. Nyide

Co-Supervisor: Dr. Mthalane

Department of Finance and Information Management

Faculty of Accounting and Informatics

Durban University of Technology

ETHICAL CLEARANCE NO: …….

- Please kindly complete this questionnaire.
- Please note that there is no correct/incorrect answer.
- Please note that participation in the study is voluntary.
- Please sign the letter of informed consent, permitting me to use your responses for this research project.
- Please kindly take note of the instructions before answering any question(s).
- Where asked for comments or to express your own opinion, keep answers short and to the point.
- Please answer all the questions as this will provide more information for the researcher so that accurate analysis and interpretation of data can be made.
- Thank you for your co-operation. The researcher hopes that you will find the questionnaire interesting and stimulating.

SECTION A: DEMOGRAPHIC INFORMATION

The following information is needed to help the researcher with the statistical analysis of data regarding the evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff. All your responses will be treated with confidentiality. The researcher appreciates your help in providing this important information.

GENERAL INSTRUCTION 1: In all the sections, kindly provide your response by ✓ making a tick ( ) in the appropriate box and fill in the gaps in the case of open-ended questions.

SECTION B: TOOLS USED BY MANAGERS TO CONTROL CYBER-LOAFING ACTIVITIES BY ADMINISTRATIVE STAFF

1.	**Age:**	☐ 18 – 30	☐ 31 – 40	☐ 41-50	☐ 51 and above

2.	**Gender**:	☐ Female	☐ Male

3.	**Ethnicity:**	☐ African	☐ Indian	☐ Coloured	☐ White
		Others (please specify):			

4.	**Academic level:**	☐ Grade 11 or less	☐ Matric	☐ Certificate	☐ Diploma
		☐ Degree	Others (please specify):		

GENERAL INSTRUCTION: In this section, please provide your response in reserved space and please give a brief explanation of your answer.

1. How do you check the Internet usage during working hours of employees in eThekwini Municipality Sizakala Customer Care?

……..……
……
……
……

2. How do you react when you walk around and observe administrative staff conducting personal business on their computers at work during working hours?

……... ……

……
……
……

3. Does your organisation have the Internet usage policy? If yes, in your opinion, do you think it is adequate to reduce cyber-loafing activities in your organisation?

……
……
……
……

4. Do you think that the Internet usage policy is clearly articulated and communicated within the organisation? Are there areas of improvements?

……
……
……
……

5. How is the Internet usage policy enforced and implemented in your organisation?

……
……
……
……

6. Does your organisation conduct awareness programmes or training on the risks and dangers of cyber-loafing? If yes, how effective are these programmes?

……
……
……
……
……

7. Do you think motivating employees to focus on their daily work can assist as a strategy to reduce cyber-loafing?

……
……
……
……

8. What are your views on blocking websites as a strategy and a way of mitigating cyber-loafing activities?

Answer:

……
……
……
……

9. Are there electronic monitoring systems used in your organisation to block employees from accessing certain websites? How effective are they?

……
……
……
……

10. Have you ever been formally informed about the abuse of internet and computer usage by the employee? If yes what was the disciplinary procedure that was followed?

……
……
……
……

11. As part of eThekwini Municipality Sizakala Customer Care Management, what are other mechanisms have you used as a way of reducing cyber-loafing among employees?

……
……
……

SECTION C: FACTORS AFFECTING THE IMPLEMENTATION OF TOOLS THAT CAN BE USED TO CONTROL CYBER-LOAFING ACTIVITIES BY ADMINISTRATIVE STAFF

12. How do you think individual habit and belief influence employees to engage in cyber-loafing?
    Answer……
    ……
    ……
    ……
    ……
13. Do you think that the daily workload that is distributed to the employees is enough to keep them throughout the day working without cyber-loafing?
    ……
    ……
    ……
    ……
    ……
14. Do you think the rise in virtual work have influence in employees to cyber-loafing?
    Answer……
    ……
    ……

……
……

15. Is your work facility conditions influence employees from engaging in cyber-loafing activities?

    Answer……
    ……
    ……
    ……
    ……

16. Do think your organisational culture encourages or leads to cyber-loafing by administrative staff?

    Answer……
    ……
    ……
    ……
    ……

17. Is cyber-loafing activities have relationship with work-related factors?

    Answer……
    ……
    ……
    ……
    ……

18. Do you think the way people are so depending to internet have influence on people to engage in cyber-loafing?

    Answer……
    ……
    ……
    ……
    ……

19. How can an organisation and their policies leads to cyber-loafing?

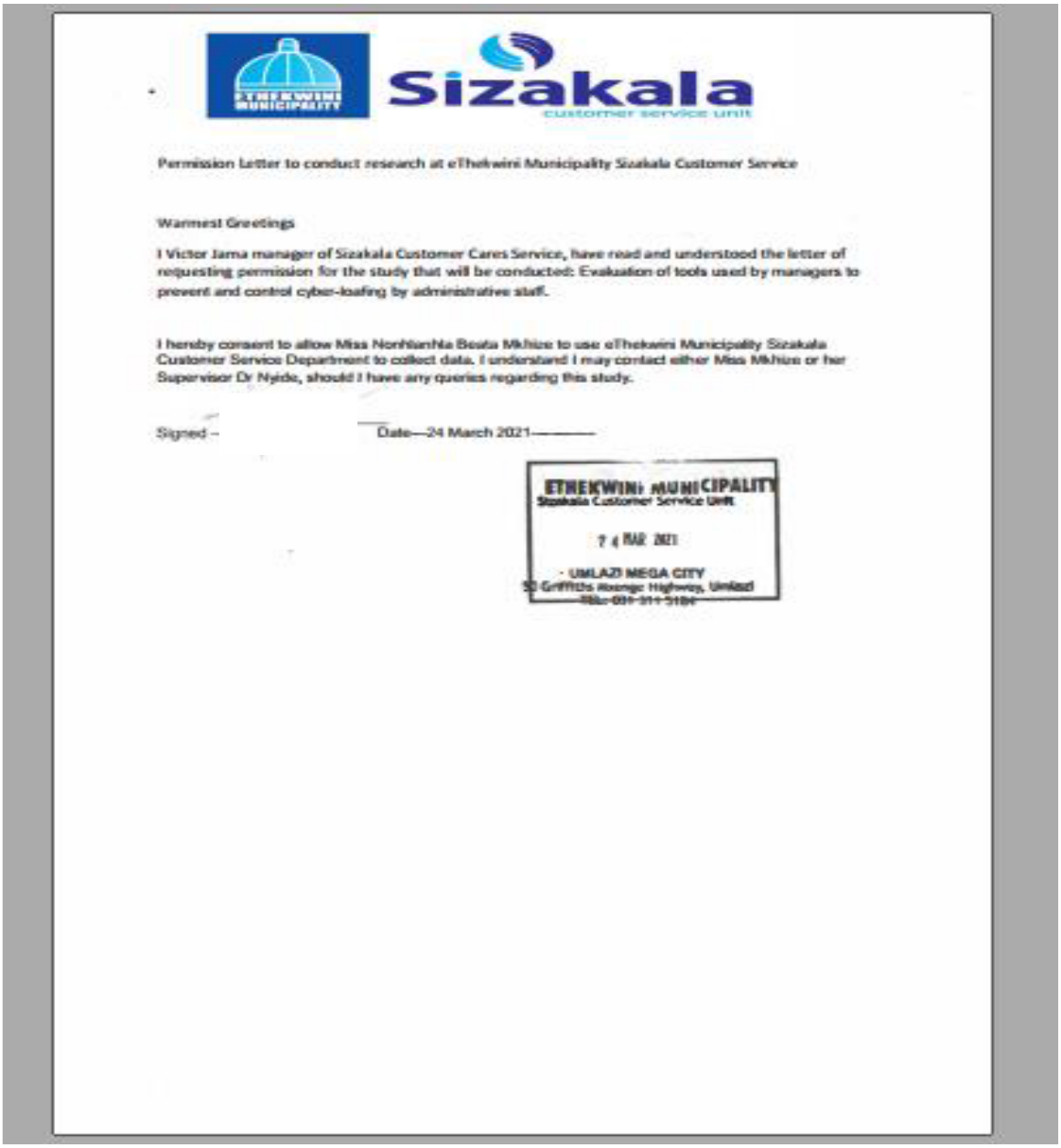
    Answer……
    ……
    ……

……

……

THANK YOU VERY MUCH FOR YOUR TIME

APPENDIX D: GATE KEEPER'S LETTER FOR ETHEKWINI MUNICIPALITY SIZAKALA CUSTOMER CARE



Sizakala
customer service unit

Permission Letter to conduct research at eThekwini Municipality Sizakala Customer Service

Warmest Greetings

I Victor Jama manager of Sizakala Customer Cares Service, have read and understood the letter of requesting permission for the study that will be conducted: Evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff.

I hereby consent to allow Miss Nonhlanhla Beata Mkhize to use eThekwini Municipality Sizakala Customer Service Department to collect data. I understand I may contact either Miss Mkhize or her Supervisor Dr Nyide, should I have any queries regarding this study.

Signed – Date—24 March 2021———

ETHEKWINI MUNICIPALITY
Sizakala Customer Service Unit
24 MAR 2021
- UMLAZI MEGA CITY
50 Griffiths Mxenge Highway, Umlazi

APPENDIX E: ETHICAL APPROVAL LETTER

Faculty Research Office
Durban University of Technology
2 July 2021

Student: Nonhlanhla Beata Mkhize
Student Number: 21101238
Degree: Master of Management Sciences in Administration and Information Management Degree
Email: 21101238@dut4life.ac.za
Supervisor: Dr CJ Nyide
Supervisor email: nyidec@dut.ac.za

Dear Ms Mkhize

ETHICAL APPROVAL: LEVEL 2
Your email correspondence in respect of the above refers.
Your proposal for a Master of Management Sciences in Administration and Information Management Degree, titled 'Evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff', was submitted to two ethical reviewers and they had the following queries:

PG2a:
The name of the qualification on PG 2a on page 1 is incorrect It should be Master of Management Sciences in Administration and Information Management.

Purposive sampling – justification?
"Sample size" – choice of number of managers, et al is not justified as per strata
Although non-probability sampling, a calculation of sample size is used (for target pop).
Despite this, 12 managers will select sample size (inconsistent and no justification)
Quantive for questionnaires and qualitative for interviews; not mentioned previously – confusing
- No interview questions provided.

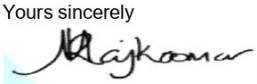
Checklist:
4: does not specify how confidentiality and anonymity will be ensured (vague)
5: stored securely and securely deleted after 5 yrs
7: more detail on the personal approach for recruit, not just distribution
16: available to participant upon request; info letter states results sent to email (inconsistent)
27: unclear benefits – may find results but no clear benefits if not acted upon
32: mentions gatekeeper letters which are not provided
33: DUT indemnity cover

Letter of Consent:
-Outline of procedure does not outline what the procedure for data collection is
- Minimal risk – if it involves humans, it is always MINIMAL or greater risk
- Non-compliance? Of the participant? Standard of care?
- Nothing on secure storage or disposal of media
- Template info still in letter

Please amend your documents as per their queries. Their decision was to resubmit to reviewers for approval of changes.

Kindest regards.

Yours sincerely



Dr Mogiveny Rajkoomar
FREC Chair
Faculty of Accounting and Informatics
Durban University of Technology
Ritson Campus
Durban, South Africa
4001

APPENDIX F: TURNITIN REPORT

Dissertation_Turnitin.docx

ORIGINALITY REPORT

10%	7%	4%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	researchspace.ukzn.ac.za Internet Source	4%
2	Dooly, Veronica Pugh. "Strategies to Monitor and Deter Cyberloafing in Small Businesses: A Case Study", Walden University Publication	1%
3	scholarworks.waldenu.edu Internet Source	1%
4	Murat Çolak, Cemile Çetin. "Loneliness and Cyberloafing in the Time of COVID-19: A Psychological Perspective", International Journal of Contemporary Management, 2021 Publication	1%
5	acikbilim.yok.gov.tr Internet Source	1%
6	Al Abbasi, Hawazin. "Organizational Information Security: Strategies to Minimize Workplace Cyberloafing for Increased Productivity.", Walden University, 2018 Publication	<1%

7	studylib.net Internet Source	<1 %
8	Submitted to University of South Africa Student Paper	<1 %
9	Hassan, Hosseini Mirza, Daraei Mohammad Reza, and Mostafa Abdol-Alivandi Farkhad. "An Experimental Study of Influential Elements on Cyberloafing from General Deterrence Theory Perspective Case Study: Tehran Subway Organization", International Business Research, 2015. Publication	<1 %
10	Submitted to University of KwaZulu-Natal Student Paper	<1 %
11	Submitted to North West University Student Paper	<1 %
12	ulspace.ul.ac.za Internet Source	<1 %
13	Kian Yeik, Koay. "Antecedents and Consequences of Cyberloafing Among ICT Employees in MSC Status Companies.", Multimedia University (Malaysia), 2018 Publication	<1 %
14	Submitted to Universiti Teknologi MARA Student Paper	<1 %
	www.fairmontstate.edu	

15	Internet Source	<1 %
16	repository.sustech.edu Internet Source	<1 %
17	vital.seals.ac.za:8080 Internet Source	<1 %
18	adoc.pub Internet Source	<1 %
19	Submitted to UNIVERSITY OF LUSAKA Student Paper	<1 %
20	Vitak, J.. "Personal Internet use at work: Understanding cyberslacking", Computers in Human Behavior, 201109 Publication	<1 %
21	digiresearch.vut.ac.za Internet Source	<1 %
22	uir.unisa.ac.za Internet Source	<1 %
23	Submitted to The British College Student Paper	<1 %
24	philpapers.org Internet Source	<1 %
25	docplayer.net Internet Source	<1 %

26	www.chp.gov.hk Internet Source	<1 %
27	Joseph, Lionel. "A framework for embedding simulation.", Sheffield Hallam University (United Kingdom), 2016 Publication	<1 %
28	cjcc.georgia.gov Internet Source	<1 %
29	repository.nwu.ac.za Internet Source	<1 %
30	Jijie Wang, Jun Tian, Zhen Shen. "The effects and moderators of cyber-loafing controls: an empirical study of Chinese public servants", Information Technology and Management, 2013 Publication	<1 %
31	Submitted to University of Venda Student Paper	<1 %
32	doras.dcu.ie Internet Source	<1 %
33	Submitted to Hofstra University Student Paper	<1 %
34	Mohmmad M. Dmour, Hanif S. Bakar, Mohammad R. Hamzah. "Antecedent, Consequences, and Policies View of	<1 %

	Cyberloafing among the Employees", Journal of Physics: Conference Series, 2020 Publication	
35	en.wikipedia.org Internet Source	<1 %
36	mobt3ath.com Internet Source	<1 %
37	www.ijss-sn.com Internet Source	<1 %
38	Submitted to American International School of Lusaka Student Paper	<1 %
39	hdl.handle.net Internet Source	<1 %
40	Submitted to Multimedia University Student Paper	<1 %
41	Submitted to University Der Es Salaam Student Paper	<1 %
42	pdfs.semanticscholar.org Internet Source	<1 %
43	umpir.ump.edu.my Internet Source	<1 %
44	Submitted to Mancosa Student Paper	<1 %
	www.emeraldinsight.com	

45	Internet Source	<1 %
46	www.ijaes.net Internet Source	<1 %
47	Rykard, Kristy Self. "Digital Distractions: Using Action Research to Explore Students' Behaviors, Motivations, and Perceptions of Cyberslacking in a Suburban High School.", University of South Carolina, 2020 Publication	<1 %
48	commons.lib.niu.edu Internet Source	<1 %
49	scholar.ufs.ac.za Internet Source	<1 %
50	ujcontent.uj.ac.za Internet Source	<1 %
51	wiredspace.wits.ac.za Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	Off		

APPENDIX G: PROOF OF LANGUAGE EDITING

Sury Bisetty Academic Editing Services

CIPC No. 2021/360666/07

The pen is mightier than the sword

To whom it may concern

I edited the thesis entitled Evaluation of tools used by managers to prevent and control cyber-loafing by administrative staff by Nonhlanhla Beata Mkhize, student number 21101238, submitted in fulfilment of the requirements of the degree of Master of Management Sciences in Administration and Information Management in the Faculty of Accounting and Informatics at the Durban University of Technology

Sury Bisetty
Professional Language and Technical Editor
02 December 2022

CONTACT DETAILS
Email: surybisetty11@gmail.com
Cell no: 0844932878 Tel.: 031 7622 766

MEMBER OF:
Professional Editor's Guild (BIS002)
South African Council of Educators (222277)
SAMEA (761237008553)

CERTIFICATION:
PEGSA: Critical Reading
Editing Mastery: How to Edit to Perfection
Complete writing, editing master class.
ELSEVIER – Editor's guide to reviewing articles

Disclaimer: Please note, I provided language and technical editing as per discussion with the client. The **content and structure** of the paper were not amended in any way. The edited work described here may not be identical to that submitted. The author, at his/her sole discretion, has the prerogative to accept, delete, or change amendments/suggestions made by the editor before submission.

NB – in keeping with POPIA regulations all work related to this thesis will be deleted 3 months after completion.