

# **CYBERETHICAL BEHAVIOUR OF HIGH SCHOOL STUDENTS IN SELECTED SCHOOLS IN UMHLATHUZE MUNICIPALITY**

**By**

**NOXOLO NQOBILE BUTHELEZI**

**A dissertation submitted in fulfilment of the requirements for the master's degree  
in Library and Information Science**

**In the**

**DEPARTMENT OF INFORMATION STUDIES**

**Faculty of Humanities and Social Sciences**

**At the**

**University of Zululand**

**SUPERVISOR: PROF. D.N OCHOLLA**

**CO-SUPERVISOR: DR. L.P. LUTHULI**

**2022**

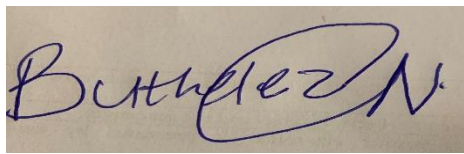
## DECLARATION

I confirm that I have read the University's postgraduate research policies and guidelines, that I understand them, and that, to the best of my knowledge and belief, I have complied with all of their requirements.

All sources and findings in this work that are not entirely my own unique thoughts have also been properly cited or referenced. The dissertation has not previously been submitted for any other degree or examination at this or any other university. I agree that my dissertation may be made accessible to the general public electronically.

Noxolo N. Buthelezi

Supervisor: Prof. Dennis N. Ocholla



Signature



Signature

Co-Supervisor: Dr Lungile Luthuli

Signature

2022

## DEDICATION

Firstly, I would like to dedicate this dissertation to the Almighty God, the one who knew me before I was born.

*“Haven’t I commanded you? Be strong and courageous. Do not be afraid nor be discouraged, For the LORD your God will be with you wherever you go”.*

(Joshua 1 vs 9)

I also dedicate this work to my late grandmother (Sizeni Albertina Ndlovu), late mother (Thembeke Gugu Ndlovu), my son (Usenathi Buthelezi), my sister (Sinethemba Khanyile), my grandfather (Bangumuzi Ndlovu) and everyone who supported me and continued to encourage me during the challenging times.

## **ACKNOWLEDGEMENTS**

A special word of appreciation goes to my supervisor, Prof. Dennis Ocholla. Thank you so much for your tireless supervision, guidance, and support. If it wasn't for your criticism and support, I would not have completed this study. It was also a pleasure to work with Dr. Lungile Luthuli as my co-supervisor. Thank you so much for pushing me all the way from my first year - now you are still guiding me.

I am very thankful to Mr Matsobane D. Kekana and Mpilo S. Mthembu, my former lecturers, for believing in me even when I had lost hope, and for your contribution to my work in some way.

To my son (Usenathi Buthelezi), thank you so much for your understanding and for coping without my presence as your mother. I am grateful for my friends' encouragement and support. My sisters and brothers from the Department of Information Studies, thank you so much for your words of encouragement and endless support.

To the Department of Education, principals from the selected high schools such as Empangeni High School (Mr. S.D. Zwane), Dlangezwa High (Mr. B.V. Gumede) and Ongoye High (Mrs. S.J. Mlenzana). Thank you so much for welcoming me warmly and allowing me to collect data at your schools. I am forever grateful.

## **ABSTRACT**

Cyber technology has become a basic aspect of schools and universities, with students' habitual use of these tools to communicate, learn, and play. However, schools and universities have faced numerous issues as a result of cyber ethics activities in various settings. This study has examined the cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality. The objectives of this study were to: explore the level of awareness of cyber ethical behaviour prevalent at the selected high schools in uMhlathuze Municipality; identify the forms of cyber ethics behaviour shown by the selected high school students; demonstrate the application of the Theory of Planned Behaviour (TPB) on cyber ethical behaviour intentions of high school students and establish the challenges faced by high school students to act ethically when using the Internet and cyber technologies. The study adopted a quantitative approach through survey research design. Probability sampling was used to sample students through the simple random technique. A sample for the study was drawn from Grade 11 students from three conveniently selected high schools in uMhlathuze Municipality. 214 questionnaires were distributed among Grade 11 students. Data was collected through questionnaires. The data analyses were carried out largely using the Statistical Package for the Social Sciences (SPSS) version 28.0.

The findings of the study show that 68.2% of the respondents were aware of their cyber ethical behaviour. Less than half (31,8%) of the respondents showed less awareness. A high percentage of the respondents (82,7%) said that their teachers hardly teach them about cyber ethics. The respondents submitted that cyberbullying (57%), using another user's password (16,4%) and dissemination of fake news (8.4%) are the common types of cyber ethical transgressions. The study discovered a substantial number of challenges related to effective cyber ethical behaviour. The findings indicated a need for awareness of cyber ethical technology and how to mitigate its misuse.

This study's originality stems from its scope, subject matter, and application. The study is significant because it provides a theoretical basis for future studies in the following areas: high schools in the uMhlathuze municipality, the levels of awareness of teachers and principals pertaining to cyber ethics. The study has implications for cyber ethical

technologies and cyber ethical behaviour in high schools' research and responses by stakeholders.

**Keywords:** *Cyber ethical behaviour, high schools, Cyber technologies, cyber ethics, uMhlathuze Municipality, Grade 11 students. TPB.*

## Table of Contents

DECLARATION .....	i
DEDICATION .....	ii
ACKNOWLEDGEMENTS .....	iii
ABSTRACT .....	iv
List of figures .....	x
Chapter 1: Introduction and background of the study .....	1
1.1 Introduction .....	1
1.2 Conceptual setting .....	2
1.2.1. Educating high school students about cyber ethics .....	3
1.3 Contextual setting .....	4
1.3.1 Dlangezwa High School .....	4
1.3.2 Ongoye High School .....	5
1.3.3 Empangeni High School .....	5
1.4. Statement of the problem .....	5
1.5. Aim of the study .....	7
1.6. Research objectives .....	7
1.7. Research questions .....	8
1.8. Significance of the study .....	8
1.10. Methodology .....	9
1.11. Definition of terms .....	10
1.11.1. Cyber ethics .....	10
1.11.2. Awareness of cyber ethics .....	10
1.11.3. Attitude .....	10
1.11.4. Cyber technology .....	10
1.11.5. Ethics .....	10
1.11.6. Cyberspace .....	10
1.11.7. Secondary school .....	11
1.11.8. Grade 11 learners .....	11
1.11.9. Computer and Information ethics .....	11
1.12. Intellectual property .....	11
1.13. Knowledge dissemination .....	11
1.14. Dissertation Research Dashboard .....	11

Chapter one: Introduction and background of the study .....	11
Chapter two: literature review and theoretical framework.....	12
Chapter three: Research methodology .....	12
Chapter four: Data analysis, presentation and interpretation.....	12
Chapter five: Discussions and findings .....	12
Chapter six: Summary, conclusion and recommendations .....	12
1.15. Summary .....	12
Chapter 2: Literature review and theoretical framework .....	14
2.2. Theoretical framework of the study.....	14
2.2.1. The Theory of Planned Behaviour.....	15
2.2.1.1. The application of the Theory of Planned Behaviour to cyber ethical behaviour intentions of high school students .....	19
2.2.1.2. Implication.....	21
2.2.1.3. The relevance of the Theory of Planned Behaviour in this study.....	22
2.3. Level of awareness of cyber ethical behaviour among students .....	23
2.4. Forms/types of cyber ethics behaviour revealed by students .....	25
2.4.1. Cyber crime.....	25
2.4.2 Cyberbullying .....	26
2.4.3. Identity theft.....	27
2.4.4. Plagiarism.....	28
2.4.5. Cyber piracy .....	29
2.5. Challenges in the efforts by high school students to act ethically when using cyber technologies .....	29
2.6. Appraisal of the chapter.....	31
2.7. Summary of Chapter two.....	34
CHAPTER 3: RESEARCH METHODOLOGY .....	35
3.1. Introduction.....	35
3.2. Research methodology.....	35
3.2.1. Research paradigm.....	36
3.2.1.1 Positivism .....	37
3.3. Research approaches.....	38
3.3.1. Quantitative research approach.....	38
3.4. Research design.....	39
3.4.1. Survey method.....	39



3.5. Target population.....	40
3.6. Sampling .....	41
3.6.1. Sample size and sampling frame.....	42
3.7. Data collection instrument and procedures .....	43
3.7.1. Questionnaires.....	44
3.8. Data analysis.....	45
3.9. Reliability and validity of the instrument.....	45
3.9. Ethical considerations.....	47
3.10. Methodological limitations.....	48
3.11. Summary of the chapter .....	48
Chapter 4: Data Analysis and Presentation of Findings.....	50
4.1. Introduction .....	50
4.2. Profiles of the participants.....	51
4.3. Awareness of cyberethical behaviour.....	52
4.4. Types of cyberethical behaviour .....	56
4.5 Summary .....	64
CHAPTER 5: DISCUSSIONS OF FINDINGS.....	66
5.1 Introduction .....	66
5.2. Profiles of the participants.....	67
5.3. What is the level of awareness about cyber ethical behaviour among students at the selected high schools in uMhlathuze Municipality? .....	67
5.4. What are the forms/types of cyber ethics behaviour revealed by the selected high school students? .....	69
5.5. How does the Theory of Planned Behaviour influence high school students' behavioural intention in Dlangezwa High, Ongoye High and Empangeni High School? .....	71
5.6. What are the challenges to the efforts by high school students to act ethically when using the Internet and computers at three selected high schools? .....	74
5.7. Summary.....	77
CHAPTER 6: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS .....	78
6.1. Introduction.....	78
6.2. Summary of findings by research objectives.....	78
6.2.1 To determine the level of awareness of cyberethical behaviour among selected high schools in uMhlathuze Municipality. ....	78
6.2.2 To identify the forms of cyber ethics behaviour revealed by the selected high school students. ....	79

6.2.3 To demonstrate the application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangezwa High, Ongoye High and Empangeni High School.....	80
6.2.4 To determine the challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools. ....	81
6.3. Conclusions.....	81
6.4. Theoretical implication .....	82
6.5. Contribution of the study .....	83
6.6. Recommendations .....	83
6.6.1. To determine the level of awareness of cyber ethical behaviour among students at the selected high schools in uMhlathuze Municipality .....	83
6.6.2. To identify the forms of cyber ethics behaviour revealed by the selected high school students .....	84
6.6.3. To demonstrate the application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangezwa -High, Ongoye High and Empangeni High School.....	84
6.6.4. To determine the challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools.....	85
6.7. Future studies .....	85
6.8. Summary.....	86
References .....	87
APPENDICES.....	106
Appendix 1: Ethical clearance letter.....	106
RESEARCH INNOVATION OFFICE .....	107
APPENDIX 2: DEPARTMENT OF EDUCATION APPROVAL LETTER .....	107
APPENDIX 3: INFORMED CONSENT LETTER.....	109
Email address : nqobileshoti@gmail.com .....	110
APPENDIX 4; PARENTAL CONSENT LETTER.....	111
APPENDIX 5: LETTER SEEKING AUTHORITY TO CONDUCT A STUDY .....	113
APPENDIX 6: DATA COLLECTION INSTRUMENTS.....	114
GATEKEEPERS FROM SCHOOLS .....	124
a) Empangeni High School.....	124
b) Ongoye high school .....	126
c) Dlangezwa high school .....	127

## List of tables

Table 1: Study population .....	43
Table 2: Awareness of cyber ethics .....	53
Table 3: Types of cyber ethical behaviour known to students .....	56
Table 4: The level of awareness of cyber technology .....	59
Table 5: Attitude toward cyber technology behaviour .....	60
Table 6: Subjective norms .....	61
Table 7: Perceived behaviour .....	61
Table 8: Influence of Behavioural Intention towards Cyber technology Behaviour .....	62
Table 9: Challenges of Cyber ethical behaviour among high school students .....	63

## List of figures

Figure 1: The theory of Planned Behaviour (Ajzen, 1991).....	17
Figure 2: Years spent in a grade .....	51
Figure 3: Cyber technology skills.....	51
Figure 4: Awareness of cyberethical behaviour .....	52
Figure 5: Teaching of cyber ethics .....	53
Figure 6: Cyber technologies in use.....	58

# Chapter 1: Introduction and background of the study

## 1.1 Introduction

Individuals are confronted with ethical issues in a variety of real-life settings, and they frequently make ethical decisions based on what they believe is right or wrong. Ethics is a concept of values that individuals live by, including what they perceive to be morally right or wrong, what they believe should be done, and what moral duties and obligations people should fulfil (Yaokumah, 2020:44). While the use of information and communication technologies helps crucial corporate processes and economic growth, it also poses ethical issues to society (Heller, 2012:34). Interactions between people and the use of digital content in cyberspace, in particular, raise ethical considerations (Jamal *et al.*, 2015:65). Some of the judgements and choices people make online are immoral or illegal (Luppigini, 2009:74). Individuals are frequently unable to settle ethical dilemmas (Yaokumah, 2020:44).

Cyberspace is a dynamic environment that is constantly creating new and contentious ethical, social, and legal problems (Aderibigbe, Ocholla and Britz, 2021:389). Cyber ethics were examined using the better-known topics of computer and information ethics as a foundation. Computer and information ethics, as part of applied ethics, can be defined as the field of study that examines the social and ethical implications of information and communication technology (ICT) (Aderibigbe, Ocholla and Britz, 2021:390). Since the early 1980s the study of cyber ethics has developed dramatically, when Johnson and Moor (1985) published important works that contributed to the discipline's definition. Since that time, the area has attracted considerable of interest from the information science community.

This study aimed to investigate the cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality and also gain knowledge of the factors that lead to such behaviour. The important factor influencing basic skills and concepts in Information and Communication Technologies in the twenty-first century is generally recognised, and many schools have included these abilities in their teaching curricula (Barakabitze *et al.*, 2019:1). The use of the Internet leads to the unethical use of cyber

technologies. Therefore, studies such as the current one is very important in bringing awareness to the use of cyber technologies.

## **1.2 Conceptual setting**

The concept of cyber ethics has attracted several definitions. According to Polkowski (2015:108), cyber ethics is the study of computer ethics, including how people use computers, what computers are programmed to accomplish, and how cyber ethics affects people and society. Cyber ethics is a concept that encompasses all types of applied ethics concerned with human actions that involve technology (Luppicini, 2009:39). Cyber ethics searches for a suitable worldview or philosophy when applying technology to actual situations (Shapiro and Gross, 2013:44).

Cyber ethics is a term used to describe ethics in cyberspace. Computing ethics is the area of applied ethics that addresses how professionals in the field of computing should make moral decisions (Polkowski, 2015:108). Thus, cyber ethics, information communication technology ethics, and Internet ethics are some of the terms used to describe computer ethics (Jamal, 2014:26). The examination of cyber ethics, sometimes known as cyber technology ethics, was built on the more advanced disciplines of computer and information ethic. As a subset of applied ethics, computer and information ethics is the field of research that examines the social and ethical implications of information and communication technologies (Bynum, 2008:32). According to Floridi (2010), It has been asserted that information ethics is the study of moral issues that are connected to one another. It is widely acknowledged that Wiener's work in the early 1940s, which led to the creation of what Wiener called cybernetics by Wiener and his colleagues, was the first to give computer ethics serious thought (Aderibigbe and Owolabi, 2020:56). In the 21<sup>st</sup> century, Information and communication technology is a tool for economic and technological progress (Aduwa-Ogiegbaen and Iyamu, 2005:22). Aduwa-Ogiegbaen and Iyamu (2005:22) recognise that despite claims to the contrary, technology has an undeniable impact on modern life and cannot be completely eliminated. A person must have a basic education to be able to access and use information in the rapidly evolving world of global market competition, automation, and growing democratisation.

### **1.2.1. Educating high school students about cyber ethics**

Teaching students about cyber ethics has become a necessity. For example, cybercrime and cyber-vandalism, which are two of the most common online concerns, can potentially affect anyone who uses the Internet or attempts to learn through the use of the Internet (Kizza, 2013:29). According to PA Media (2020), for the majority of young people, electronic devices have become an integral part of their lives. Many people report being afraid of living without their phones, and more than half of them sleep with them next to their beds. PA Media (2020) admits that since a mobile phone is a private technology that is kept, literally, close to the chest, it can be difficult to monitor what the child is viewing online. Admittedly, we live in a linked world with a wealth of valuable Internet platforms for learning and peer cooperation, which is undeniable. However, the flip side of the coin must be considered: identity theft, cyberbullying and phishing scams are all too common. In order to prevent younger students from slipping into internet traps, cyber ethics education should be taught in high schools. According to Rasmitadila *et al.* (2020:91) due to modifications in educational systems, schools are now required to offer online education, correspondence education, extracurricular activities, adaptable learning, and massive open online courses (MOOCs). Increasing access to education as well as equity, quality, and the relevance of education globally has been positively impacted by the development of digital technologies and the Internet (Power, 2014:91).

The study by Sahin, Balta and Ercan (2010: 234) noted that the use of the Internet, particularly in education, has been studied for a while, and there are numerous studies on the topic in subject literature. The most powerful communication resources, social media and the Internet have become a part of the daily routine and one of the most significant educational tools. Because the Internet facilitates the dissemination of materials between diverse sites, it is an extremely strong information service. The question of whether the mentioned source is reliable and/or reputable has been raised, despite the fact that the Internet is a highly essential and indispensable source for students (Sahin, Balta and Ercan, 2010:236). They also point out that, unlike scientific and professional periodicals produced by research institutions, the corporate sector, and

well-known organisations, there is no control over every single piece of information published over the Web.

### **1.3 Contextual setting**

The study was conducted at King Cetshwayo district under uMhlathuze local municipality from the three selected high schools in the KwaDlangezwa and Empangeni areas. uMhlathuze Municipality is the third-largest municipality in KwaZulu-Natal; it is located on the northeast coast of KwaZulu-Natal. The city of uMhlathuze comprises the townships of Ngwelezana, Felixton and Mandlanzini, and rural areas which are under the traditional authorities of KwaDlangezwa (under inkosi uMkhwanazi), Obizo (inkosi Cebekhulu), Buchanana (inkosi uMthiyane) and KwaBhejane (inkosi Khoza). Although it is situated in a rural area, the municipality currently has a few significant industrial growth points. The municipality is divided into 34 wards and is home to the continent's deepest harbour as well as ample territory for heavy-duty enterprises. About nineteen secondary high schools exist within the area and they are either private schools or state-supported schools.

#### **1.3.1 Dlangezwa High School**

Dlangezwa High School is known as a girls' high school; it is located within King Cetshwayo District in uMhlathuze local municipality in KwaZulu-Natal. A teacher by the name of Dr. Sibusiso Bhengu founded it in 1969. He spent seven years as the school's first principal and put all his passion into turning Dlangezwa into a top-performing institution. It was a place of excellence and great accomplishment. Dlangezwa High School has been a proud high school for its entire 50-year existence. One of the brave regiments of King Shaka ka Senzangakhona, the founder of the Zulu Nation, was called Dlangezwa.

Dlangezwa High School is an all-girls secondary boarding school with a Christian ethos. Currently, there are 37 teachers and 872 students enrolled. Mr S.K Mthiyane is the principal of Dlangezwa High. It is a public institution in King Cetshwayo and specialises in ordinary school education. Dlangezwa High is a fee-paying school. It provides a rich learning atmosphere in which numerous students have been able to study, develop, and

grow. The curriculum and instructional methods assist students in taking the next step in their study and fearlessly facing the future.

### **1.3.2 Ongoye High School**

Ongoye Secondary School is located in KwaZulu-Natal within King Cetshwayo district in uMhlathuze local municipality. There are 32 teachers, and 740 learners enrolled. Ongoye is a rural public secondary school in a rural suburb at KwaDlangezwa; it enrolls learners from Grade 8 to Grade 12 and is listed as a free institution in quintile three. From Grade 10 to Grade 12, they offer Physical science, Life science, Mathematics, Mathematics Literacy, Accounting, Business Studies, Economics, Life Orientation, History, Agricultural Science and Geography, first additional language, and IsiZulu home language.

### **1.3.3 Empangeni High School**

Empangeni High School was established in 1957, the largest and best-known high school in Zululand. The new structure, which was completed in 1975, is located next to the previous one. The school is home to well-equipped Life and Physical Science laboratories, a contemporary mechanical workshop, consumer study centres, computer and IT centres, and an Engineering Graphic Design department that is fully functional.

The school has a large sports field and a modern, well-equipped school building complex. The educators are committed to their work and ensure that all students are guided through a curriculum that allows them to achieve their full academic potential in a variety of subjects. Matriculants in 2018 had a 97 per cent pass rate, with 217 matriculants earning 263 distinctions and 144 bachelor's degrees. Each student is encouraged to display their abilities in a warm, traditional, and healthy environment. Cricket, rugby, hockey, swimming, tennis, soccer, volleyball, netball, and squash are among the sports offered, with many students selected to present Northern Coastal, KZN and ZLD teams.

## **1.4. Statement of the problem**

In the 21<sup>st</sup> century, information and communication technologies play a huge role in the development of modern societies. Rapid developments in cyber technology have resulted



in the development of laws and rules; however, not all users of these technologies are aware of or informed about these laws and rules. It is critical to improve public awareness about the importance of ethical issues surrounding cyber technology. In recent years, African high schools and institutions have developed computer use rules that address various aspects of cyber technology use, copyright and other ethical concerns. Aderibigbe (2019:10) has noted that the use of such technologies is governed by ethical norms, which act as gatekeepers and, to some extent, deter ethical transgressions. High school learners, on the other hand, are unaware of these ethical principles. Moor (2001) indicated that the students' lack of understanding, knowledge, and awareness of cyber technology ethics leads to decisions made without regard to ethical responsibility and use.

The study by Udo-Akang (2013:59) has revealed that the increasing commercialism of the Internet and the growth of websites has spawned a new breed of intellectual property ownership rights; concerning trends in recent years include software privacy, counterfeiting in movies, music, videos, books, and images, an information utilisation chain among other vices. Aderibigbe (2019:10) emphasised that these unethical cyber behaviours have become frequent among students, and many of them have ramifications for their careers in the larger business world. However, a study by Acilar and Aydemir (2010:4) of prospective supervisors and workers' attitudes concerning ethical computer usage found that students who use cyber technology are more likely to engage in unethical activity.

Among identified gaps in the literature, the current study was triggered by Aderibigbe's (2019:11) view that in Africa, cyber ethics has a dearth of ethical research applications, and the pattern of unethical research behaviour is relatively recent. There has not been much written about the effects of Information and Communication Technology (ICT) on African societies or how to utilise it ethically (Capurro, 2008:103). The usage of the Internet by high school students is currently posing challenges to cyber ethics. It is critical to improve student knowledge of the importance of ethical problems surrounding cyber technology in schools. Intellectual property offenses, copyright infringement, digital piracy, and plagiarism are a few of these illicit behaviours (Aderibigbe, 2019:10). The

latest generation of intellectual property problems, brought on by the Internet's ongoing commercialization and the proliferation of websites, clearly represent dishonest business practices and violations of the ownership rights of intellectual property along the value-adding chain of information. In recent years, a number of vices including software theft, counterfeiting of movies, music, videos, books, and artwork have grown alarming. (Rujoiu and Rujoiu, 2014; Udo-Akang, 2013). Failure to identify solutions to this problem of unethical use of cyber technology can lead to more cyberbullying and children committing suicide because of the things that have been said about them in cyberspace. It is essential to teach high school students about information ethics and bring awareness of their cyberethical behaviour when using cyber technologies. This research is likely to add to the body of information currently in existence and knowledge in the field of cyber ethics and to raise awareness of learners' unethical usage of cyber technology in the classroom.

### **1.5. Aim of the study**

The study aimed at examining the unethical cyber behaviour of high school students in the three selected schools in uMhlathuze Municipality and gaining knowledge of the factors that led to such behaviour.

### **1.6. Research objectives**

The following objectives were set:

- To determine the level of awareness of cyber ethical behaviour among the selected high schools in uMhlathuze Municipality.
- To identify the forms/types of cyber ethics behaviour revealed by the selected high school students.
- To determine the application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangezwa High, Ongoye High and Empangeni High School.
- To establish the challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools.

## **1.7. Research questions**

The subsequent research questions provided for a thorough understanding of the study's research problem:

- What is the level of awareness of cyber ethical behaviour among the selected high schools in uMhlathuze Municipality?
- What are the forms/types of cyber ethics behaviour revealed by the selected high school students?
- How does the Theory of Planned Behaviour influence high school students' behavioural intention in Dlangezwa High, Ongoye High and Empangeni High School?
- What are the challenges to the efforts by high school students to act ethically when using the Internet and computers at three selected high schools?

## **1.8. Significance of the study**

Cyber ethics in high schools is becoming more important as students are becoming more exposed to using technology. Students need to be taught how to recognise their positions in the social network environment, along with the power of a single post. Theory of Planned Behaviour (TPB) was chosen as the study's underpinning framework, and so contributes to the body of knowledge because it combines personal normative and controls aspects that may influence the purpose that dictates behaviour in cyberspace. A variety of behavioural intervention studies have employed the Theory of Planned Behaviour (TPB). However, in high school-based cyber ethics classes, it has not been used much. The study concentrated on the selected high school students in uMhlathuze. It was significant in the sense that it disclosed the hidden attitudes of a selection of high school students concerning the use of cyber technology and improper Internet use. This study analysed selected high school students in the uMhlathuze Municipality's awareness of cyber ethical behaviour, and also informed them about the use of Information and Communication Technology (ICT) when retrieving information in cyberspace for academic purposes. It is important that high school students are taught about information ethics at the early age group as they start using cyber technologies at a very young age.

## **1.9. Scope and limitations of the study**

The scope of the study was strictly limited to the three selected high schools in uMhlathuze Municipality, namely Dlangenzwa High, Ongoye Secondary and Empangeni High School. Even though the study recognizes the presence of other academics and their use of cybertechnology, its main focus only includes grade 11 students. The study's theoretical framework is the Theory of Planned Behaviour, which focuses on cyber ethical behaviour and unethical use of cyber technology. It covered only the subject area of information ethics in business studies. In order to have a thorough grasp of the research problem from the chosen schools, the researcher used the quantitative research methodology for the study, which was conducted in a positivist paradigm. The three schools under uMhlathuze Municipality were chosen in order to compare the township high schools with multi-cultural public schools that are based in town. Both high schools are under government, but they are situated in different wards.

## **1.10. Methodology**

The study has applied Theory of Planned Behaviour (TPB) as a theoretical framework (as discussed in detail in Chapter two). According to Goundar (2012:10), research methodology is defined as a systematic approach to problem-solving. This is a science that studies how to conduct research (Goundar, 2012:10). However, Ngulube (2015:34) describes methodology as primarily concerned with how information is comprehended, distinct, analysed, confirmed, mediated, appraised, discovered, studied and understood. The study adopted a quantitative approach. The positivist paradigm was adopted, and a survey design using a questionnaire as the data collection tool was employed. The study's questionnaire was deemed to be the greatest tool as it spared the study's participants' time. It was distributed among Grade 11 learners in Dlangenzwa High, Ongoye High as well as Empangeni High School. The learners were selected using random sampling. Therefore, each learner had a chance of being selected. The chosen design and method examined and analysed what is naturally occurring in the researched context, as well as the creation of a picture of the situation at hand. Detailed information about the research methodology will be found in Chapter 3.

## **1.11. Definition of terms**

This section provides major concepts used in this study.

### **1.11.1. Cyber ethics**

Bawa and Marwah (2011:54) define cyber ethics as the study of ethics that is about computers and what computers are programmed to do, as well as how it affects society. Cyber ethics is based on codes that guide proper Internet behaviour for the benefit of individuals and society.

### **1.11.2. Awareness of cyber ethics**

Understanding and access to information regarding how the Internet can be used in various circumstances is referred to as cyber ethics awareness. It entails being exposed to the norms that govern cyberspace. Therefore, cyber ethics education must be provided to students by schools and colleges (Milton *et al.*, 2021:21). Understanding the importance of cyber ethics in daily life has become more important than ever before.

### **1.11.3. Attitude**

In this study context, attitude reflects the favourable or unfavourable appraisal of students' engagement with illegal downloading of music or films and using cyber technology in an unethical manner. Students who support unethical online behaviour are more likely to engage in digital piracy and other improper uses of technology.

### **1.11.4. Cyber technology**

Smartphones, tablets, and personal computers are just a few examples of the many computing and networked communication devices that fall under the umbrella of "cyber technology" (Aderibigbe, 2019:10). Anything that is connected to the Internet is regarded as cyber technology.

### **1.11.5. Ethics**

Ethics are referred to as the rules and principles that assist one in differentiating between right and wrong.

### **1.11.6. Cyberspace**

Cyberspace is the term that describes the environment where there is widespread interconnected digital technology (Mbanaso and Dandaura, 2015:18).

#### **1.11.7. Secondary school**

Students in secondary school, also known as senior high school, range in age from 13 to 18 years, after primary school and before higher (post-school) institutes of learning, which follows studying at secondary school (Maphoto, 2016:11). It offers students the secondary education they require in order to pursue further education.

#### **1.11.8. Grade 11 learners**

Refers to the learners that are preparing themselves for Grade 12.

#### **1.11.9. Computer and Information ethics**

The phrase refers to the area of applied ethics that investigates and assesses the social and ethical implications of ICT.

#### **1.12. Intellectual property**

The dissertation remained the property of the University and as such, it was deposited in the institutional repository at the University of Zululand library and copies were made for the three selected high schools in uMhlathuze Municipality.

#### **1.13. Knowledge dissemination**

Findings from the study were published as a dissertation in the University of Zululand's institutional repository, which is open to the public. The research's findings were also shared with the University of Zululand's library. Other study findings were disseminated through research articles published in peer-reviewed journals.

#### **1.14. Dissertation Research Dashboard**

The dissertation consists of six chapters, as follows:

##### **Chapter one: Introduction and background of the study**

The study contextualised and conceptualised the research on the cyber ethical behaviour of high school students in the selected schools in uMhlathuze Municipality. By introducing and outlining the context of the study, the chapter establishes the groundwork for the remaining chapters. The conceptual framework, problem description, study objectives, and particular research questions that the research questions were intended to address are also presented. After discussing the study's significance and limitations, the study's scope is discussed. It goes on to explain the research methods, ethical issues, and the study's organisational structure.

## **Chapter two: literature review and theoretical framework**

Chapter two reviews literature about the study, discusses the theory that was used in accordance with the study's research objectives and examines the cyber-ethical behaviour of high school students. The study discusses types of cyber ethics behaviour revealed by the selected high school students such as cyberbullying, hacking, cybercrimes as well as cybersecurity.

## **Chapter three: Research methodology**

Chapter three discusses the research strategy utilised to address the study questions. The chapter also provided an overview of the quantitative research methodology. The researcher used questionnaires to gather data. The quantitative data was investigated using statistical data analysis.

## **Chapter four: Data analysis, presentation and interpretation**

Chapter four provides and evaluates the information that was intended to investigate the cyber ethical behaviour by high school students at the three selected schools in uMhlathuze Municipality. The study's findings provided complete answers to the main research topics. The chapter concludes with a discussion of issues and suggestions for how high schools might address them to raise students' awareness of cyber ethics.

## **Chapter five: Discussions and findings**

After data analysis, chapter five analyses the conclusions revealed in chapter four.

## **Chapter six: Summary, conclusion and recommendations**

The final chapter of the research report comes to an end here. It includes a summary, recommendations based on the study's findings, and conclusions. There will also be recommendations for future research.

### **1.15. Summary**

Since students routinely utilise these technologies to communicate, learn, and socialise, cyber technology has become an essential component of educational institutions, including secondary schools. This necessitates the adoption of ethical computing practices in academia. One of the biggest issues that are facing learners is how to access information without violating any ethical rules. This chapter addresses the research

background and overview of cyber ethics as an area and types of cyber ethics. The problem statement, aim and objectives of the research were discussed. The chapter further provided the methodological scope and limitations of the current research. The scarcity of research on cyber ethical behaviour in high schools was pointed out, and the gap which the study sought to fill was established. The Theory of Planned Behaviour (TPB) was adopted to analyse and examine the learners' intentions and attitudes. Understanding learners' cyber ethical intentions and behaviours will help to inform the management of schools on what tools should be used to guide ethical conduct. The next chapter reviews existing literature on cyber ethical behaviour.



## **Chapter 2: Literature review and theoretical framework**

### **2.1. Introduction**

The study's introduction and context were covered in the previous chapter. This chapter examines the literature on cyber ethical behaviour. Ridley (2012:48) states that a literature review is defined as "an exhaustive reading for linked research and theory about one's field of interest." The literature review connects the researcher's thoughts with those of other researchers. This starts by exploring the theory underlying this study and highlighting the results of studies in the area of cyber ethics. The chapter begins with discussing the study's conceptualisation. The literature review for this research focuses on the following themes:

- level of awareness of cyber ethical behaviour among the selected high schools in uMhlathuze Municipality.
- forms of cyber ethics behaviour revealed by the selected high school students.
- application of the Theory of Planned Behaviour on the cyber ethical behaviour intentions of high school students in Dlangenzwa High, Ongoye High and Empangeni High School.
- challenges faced by high school students to act ethically when using the Internet and computers at the three selected high schools.

The theoretical foundation of the study is covered in the following section.

### **2.2. Theoretical framework of the study**

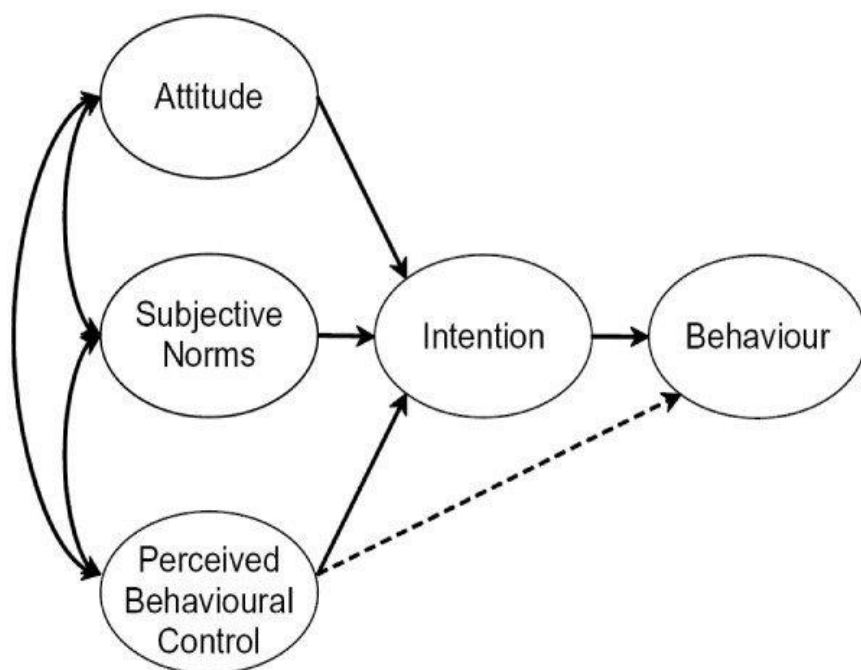
The theoretical framework acts as the cornerstone on which a research study's body of knowledge is created (Osanloo and Grant, 2014: 12). As a result, a conceptual framework provides background information regarding a researcher's field of study. According to Ledwaba (2018:31), the theoretical model forms the study's backbone, considering its relationship to previous related applications. The importance of a theoretical framework to the research study cannot be overstated because it directs the research operations with the aid of a formal theory (Ocholla and Le Roux, 2011:61). Mintzberg (2017:179)

claims that a good theory should be functional, strong, parsimonious and valid. Therefore, the theory serves as the backbone of the research as it should resemble the study objectives and questions of the study. It is important to evaluate and discuss the model that is relevant to the cyber ethical behaviour of high school students in the selected high schools in uMhlathuze Municipality. Therefore, this study made use of Icek Ajzen's Theory of Planned Behaviour, which was first proposed in 1985, to explore unethical cyber behaviour among high school students at the three chosen schools in the uMhlathuze Municipality as well as high school students' opinions towards the use of cyber technology.

### **2.2.1. The Theory of Planned Behaviour**

According to Ajzen, (1991:180), a crucial component of the notion of planned behaviour is the person's motivation for engaging in a certain behaviour. Hence, it is considered that preferences encapsulate the inspirational variables that impact behaviour. They demonstrate a person's level of commitment to the behaviour and the amount of effort they plan to put in (Ajzen, 1991:181). Social, psychological and knowledge factors have been shown to influence an individual's cyber ethical decision. According to Ajzen, (2011:115), the TPB is interested in predicting intentions, subjective norms, and perceptions of behavioural control are all assumed to have an impact on and provide an explanation for behavioural intents. According to the hypothesis of arranged conduct, a person's behavioural eagerness is directly impacted by demeanours, subjective standards, and PBC, though deliberate behaviour is thought to be the most grounded indicator of genuine conduct (Ajzen, 1991). It is genuine, that the hypothesis of arranged conduct is concerned with the controlled components of human data handling and decision-making. To defend this, Ajzen (2011:116) is largely concerned with goal-directed behaviour which is guided by cognisant self-regulatory frameworks. This accentuation has been misinterpreted to demonstrate that the hypothesis expects an impartial, enthusiastic on-screen character who assesses all pertinent data before making a behavioural decision (Ajzen, 2011:1116). In actuality, the idea paints a far more detailed and intricate picture.

According to Ham, Jeger and Ivkovic (2015:739), the Theory of Planned Behaviour expects that most human conduct is the result of people craving to lock in a certain conduct and his or her capacity to create a cognisant choice almost achieves it. Whether eagerly anticipated conduct is impacted by circumstances beyond the individual's control, i.e., the quality of the expected conduct relationship is balanced by genuine control over the conduct. Therefore, it is more likely that a deliberate intention to lock in a behaviour will be carried out the more solidly it is based. It have been widely used in a variety of studies on social and human behaviour, especially those that focus on moral issues, such as those involving cyber technology (Attuquayefio and Addo 2014; Goles *et al.*, 2008; Taylor and Todd 1995), advanced piracy (Liao, Lin and Liu 2010; Yoon 2010), unethical behaviour (Chatterjee, Sarker and Valacich, 2015), awareness of cyber innovation morals (Chiang and Lee 2011 (Harding *et al.*, 2007). Despite this, there are numerous critiques of the theory, though not necessarily legitimate and fair. It seems the theory is constrained by questions of usefulness and generalisability (Head and Noar, 2014). However, the theory has demonstrated its effectiveness in describing a wide range of behaviours after taking into consideration a variety of moderating influences (McEachan *et al.*, 2011). The components of the theory are presented in Figure 1 and discussed below.



**Figure 1: The theory of Planned Behaviour (Ajzen, 1991)**

The association between the state of mind toward the behaviour, subjective norm, seen behavioural control, and behavioural intention is shown in Figure 1. All of these elements combine to impact students' willingness to lock in computerised piracy and unethical cyber technology use.

## Attitude

Attitude towards behaviour is how much a person's presentation of conduct is decidedly or contrarily esteemed. As indicated by Ajzen (1993:44), an attitude is a person's appearance to respond with a specific level of favourableness or unfavourableness to an article, conduct, individual, or occasion. Although format definitions of attitude differ, most contemporary theorists concur that attitude's evaluative nature is its defining trait. (Fishbein and Ajzen, 1975, Edwards, 1957 Oskamp, 1977). This view is reinforced by the way that practically all standard mentality scaling methods bring about a score that regards a person on an evaluative continuum (Ajzen, 1993:41). People's attitude varies from belief in that it shows a particular attitude toward the focus of interest. Subsequently, an individual's opinion about cyber ethics behaviour may shift from antagonistic too optimistic on a scale (Aderibigbe, 2019:27). Thus, attitude is a result of a person's

behavioural beliefs, which describe the behaviour's likely outcomes (Conner, 2001). Cronan and Al-Rafee (2008) and Liao, Lin, and Liu (2010) found that a figure of advanced piracy and untrustworthy cyber behaviour among the inspected populace is the behavioural deliberate, characterised as the user's readiness to carry out a certain conduct (Ajzen 1991).

## **Subjective norms**

According to Fishbein and Ajzen (2005:27), the social pressure or perceived social pressure to perform or not execute a particular behaviour is referred to as the subjective norm. Subjective norms refer to the belief that a well-known individual or number of individuals would endorse and uphold a specific behaviour (Ham, Jeger and Ivkovic, 2015:744). Subjective norms are defined as the expectation that a significant person or group of people will approve of and support a certain behaviour (Ham, Jeger and Ivkovic, 2015:740). Furthermore, subjective norms are defined by an individual's desire to conform to others' views and their perception of social pressure from others to conduct in a specific way. One possible explanation for the subjective norms variable's inconsistency in importance is that a portion of the information included in this variable is already available in the wanted capacity carrying out a specific behaviour variable. Moreover, it is assumed that the antecedent of subjective norms is a function of beliefs, but of a different kind from the first antecedent: the person's beliefs that particular people or groups endorse or oppose carrying out the behaviour, or that these social groups of interest themselves engage or do not engage in it. The seeming prevailing pressure from others for a person to behave in a specific manner and the inspiration to comply with those individuals' viewpoints, decide these. However, the impact of subjective norms on cyber technology expectations ends up being by and large more fragile in past examinations than the influence of attitude (Taylor and Todd, 1995:55). According to Neighbors and Fossos (2013:323), they use important people solely as their reference group, and the conduct of relevance is focused on the perceiver's behaviour instead of generic activity. However, this isn't to say that peer influences aren't essential; they are, but they are less prominent and far less likely to be targeted on addictive behaviours. Subjective norms allude to an individual's impression of societal weights from others who

matter to them (e.g., family, companions, co-workers, and others) to act (or not act) in a certain way, as well as their motivation to take other people's suppositions (Ham, Jeger and Ivkovic, 2015:743). Perceived behavioural control is the final important interpreter which remains also influenced by beliefs.

### **Perceived behavioural control.**

These variables reflect whether or not a person actually has control over a behaviour (Bisquolm, 2010:05). According to Ajzen and Fishbein (2005:181), perceived behavioural control is seen as the capacity that a person has to wilfully participate in a specific behaviour. It speaks of a person's perception of the simplicity or trouble of playing out the behaviour of attention. Students will intend to engage in negative cyber ethics behaviour when they have decided to do so, when they are having difficulty doing so, and when they believe they have the tools and flexibility to do so (Ajzen, 2005:37). Given the prevalence of the issue, the ideal way to define a behavioural intention is as an intention to attempt to engage in a particular behaviour (Ajzen, 2005). Exemplary behavioural control is described by confidence in a person's capacity to effectively achieve an ideal assignment (for example, advanced robbery and dishonest utilisation of cyber technology) (Ajzen, 2005:36). Furthermore, Aderibigbe (2019:29) emphasises that students' opinions about their capacity to control factors in their current situation that either work with or restrain their ability to engage in unethical cyber behaviour are influenced by their previous experiences with computerised theft and dishonest use, as well as their perceptions of their ability to regulate variables that either work with or restrain their capacity to act unethically online. Therefore, the Theory of Planned Behaviour (TPB) has been employed as an intervening theory in this study to evaluate the cyber ethics behaviour of a selected high school in uMhlathuze Municipality.

#### **2.2.1.1. The application of the Theory of Planned Behaviour to cyber ethical behaviour intentions of high school students**

The Theory of Planned Behaviour (TPB) is undoubtedly one of the most widely studied and applied in the field of research on human behaviour. The theory of planned behaviour

has now been extensively applied and enlarged to research individual behaviour, particularly in the prediction of outcomes, for the previous two decades. It is the deliberate intention of a person to act and genuine behaviour. Based on Ajzen and Fishbein (1980:204), the theory of planned behaviour (TPB), is founded on an individual's intention (motivation) to engage in a given activity; the stronger the intention, the more likely the behaviour will be engaged. According to Lin and Chen (2011:66), the idea of reasoned action states that intention is the individual's intention to perform, which is always under individual control. Furthermore, attitudes toward the behaviour and subjective norms both have an impact on one's motivation to perform a specific action. The theory was expanded in order to forecast behaviours that an individual might not be able to carry out on their own (Ajzen, 1985; and Ajzen, 1991). Since then, the model has been applied to numerous behavioural studies in a range of disciplines.

Bisquolm (2010) states that intentions are a function of three fundamental determinants, in the theory of planned behaviour so these three are concerned with control issues: one is personal in character, one reflects social pressure and influence. Perceived behavioural control is a very good predictor of such acceptance. He adds that "the notion of planned behaviour has proven to be helpful in anticipating technological uptake." According to the Theory of Planned Behaviour, intention and behaviour are influenced by perceived behavioural control. These claims were refuted by a study done in 2019 by Aderibigbe (2021:223), which showed that access to a large amount of information on the Internet has been made available by cyber technological advancements made on university campuses, which has advantages and disadvantages for both institutions and students. Stone *et al.* (2010) employed structural equation modelling to show that there is a connection between perceived behavioural control and intents, as well as the use of cyber technology, when examining the relationship between these two variables.

Similar discrepancies between subjective norms and people's actual intents have been discovered in earlier research on the TPB (Peng, Zhu, Tong, and Jiang, 2012; Bouhnik and Deshen, 2014). This, however, confirms the findings of Armitage and Conner (2001) and Taylor and Todd (1995), which suggest that subjective norms, as an independent variable, have a shaky influence on how people misuse cyberspace. Alternatively, it could

simply mean that students may be motivated to act immorally in the pursuit of thrill and attention, which may simply override the impact of significant others, because of the anonymity of the Internet, which creates a strong feeling of being able to act freely without fear, and independently of significant others.

#### **2.2.1.2. Implication**

The reviewed literature on the Theory of Planned Behaviour, which was used in this study, demonstrates that ethical practice is still a major concern across many fields of study on a worldwide scale. Unethical use of cyber technology aimed at high school students seems to be high and they are not always aware of the rules and regulations of cyber ethics. The study aimed at examining the unethical cyber behaviour of high school students in the three selected schools in uMhlathuze Municipality and at gaining knowledge of the factors that can lead to such behaviour. Therefore, to research this phenomenon, the study used a hypothesis framework to seek insight into how young adults actually behave ethically when using technology as well as to develop an intervention to stem the flood of improper practices. By creating a behavioural process model and evaluating the applicability among its implementation in emerging regions where unethical cyber behaviour is apparent, this analysis has contributed to the literature on cyber ethics behaviour. According to Molnar, Kletke and Chongwatpol, (2008), per the studies, unethical behaviour in school systems is connected to an unethical cyberethical mindset at work.

The results of Ajzen's study (1985, 1991) are supported by the empirical information reported in this research; the Theory of Planned Behaviour can forecast cyber behaviour and provide recommendations for potential ethical applications of cyber technology inside the classroom context. The study's significance for education systems is clear: it aims to stop unethical cyber behaviour. It serves as a valuable manual for developing curriculum interventions and policies. These should pay attention to and concentrate resources and efforts on enhancing students' understanding of moral decision-making and conduct in cyberspace. Students can easily comprehend opposing viewpoints and make more well-informed choices about the use of telecommunications by being aware of potential complications and ethical dilemmas through cyber technology ethics (Acilar and Aydemir,



2010). More discussion boards, where stakeholders' nuanced views on what creates cyber ethics behaviour and how to think and act in cyberspace can be held, are required to be initiated by school principals and teachers.

#### **2.2.1.3. The relevance of the Theory of Planned Behaviour in this study**

This study examined which of the Theory of Planned Behaviour's components accounts for high school students' behavioural views regarding cyber technology. Numerous behaviours have been subjected to the Theory of Planned Behaviour in an effort to better comprehend who exhibits specific behaviours. It has been cited as one of the most influential social behavioural and cognitive decision-making theories, as well as one of the socio-psychological theories having the best evidence for predicting human behaviour (Sommer, 2011). There is acceptance that the Theory of Planned Behaviour is assumed to utilise the foundation for interventions in cyber ethics behaviour. In a sequence to determine and evaluate the impact on behaviour, the theory first postulates distinct constructions. Second, research in information studies frequently uses the Theory of Planned Behaviour (Godin, Conner, and Sheeran, 2005 and Ogden, 2003). It is one of the most popular social cognition models. Third, meta-analyses of correlational studies based on the Theory of Planned Behaviour have offered empirical support for its ability to identify and examine a variety of behaviours (Armitage and Conner, 2001; Conner and Sparks, 2005), including unethical cyber behaviour (Liao, Luo, Gurung and Li, 2009; Aderibigbe, 2021).

Researchers have utilised the notion of reasoned action as a model to look at users' behaviours before the Theory of Planned Behaviour was developed. But the robustness of the theory and the postulation of the Theory of Planned Behaviour resulted from the addition of the perceived behavioural control construct to the theory of reasoned action. The idea is a well-known social psychology concept that has been used to explain a variety of phenomena connected to human behaviour. The Theory of Planned Behaviour may be employed to evaluate students' perceptions of control over engaging in the target behaviour, normative attitudes, and cyber ethics behavioural beliefs (digital piracy and unethical use). In particular, it is very likely that a student will utilise cyber technology unethically and indulge in digital piracy if they have a favourable attitude toward doing so,

if significant referents have positive expectations of them that they should comply, and if they believe they have complete control over carrying out the intended behaviour. In contrast, they will refrain if the results of engaging in this target behaviour are perceived adversely or unfavourably and the student feels under social pressure from significant others to disobey. Additionally, non-compliance behaviour is very likely to occur if there are no real constraints to it.

The next section reviews literature in the domain guided by the themes from the study objectives.

### **2.3. Level of awareness of cyber ethical behaviour among students**

Kortjan and von Solms (2013:291) note that cyber ethics awareness and training is essential for moral execution on the Internet. Ngoqo and Flowerday (2014) conversely consider mindfulness and information as two significant variables of digital innovation conduct goals of understudies in higher foundations in South Africa. Aderibigbe (2019:46) sees awareness as a prerequisite to the mentality arrangement phase of digital moral expectation and conduct. According to the framework and setting of this study, this would imply that awareness is a prerequisite for attitudes and behavioural intentions. According to Aderibigbe (2019:46), citing Trevino, Weaver, and Reynolds, it is the understanding of a person that his or her potential decision or action may have an impact on the interests, welfare, or expectations of self or others in a way that may be inconsistent with one or more ethical standards. Therefore, awareness is defined as the capacity to be aware of situations that could present an ethical conundrum when using cyberspace and cyber technology. The relevance of cyberspace has increased for a country's residents, enterprises, and overall economy, claim Kortjan and von Solms (2013:289). They go on to say that a country should take the initiative in Internet security. However, it is crucial to advance cyber security knowledge and education given the inherent difficulties.

Most studies on the use of educational technology in high schools concentrate on how it is implemented and how it affects the learning environment (Ozer, Ugurlu and Beycioglu, 2011:17). Similarly, younger children have raised more questions in society about who should be in charge of educating them on how to use technology responsibly (Yamano

and Jayne, 2004:98). The Internet's unique qualities and its ability to connect people in communities with the outside world have received attention on many of the ethical questions surrounding the use of and exploitation of the advantages of various cyber technologies (Aderibigbe, Ocholla and Britz, 2021:390). The use of computers has changed the way people teach and learn, improving accessibility, independence, interaction, and enthusiasm for learning. According to Oyewole (2017:69), university students in the 21<sup>st</sup> century cannot be acquired through society's evolution without the aid offered by computers. The growth of the Internet and the world-wide web has made this easier. Oyewole (2017) states that the majority of the intriguing research examined the degree of student understanding of their beliefs regarding computer ethics, with some also taking gender into account.

The perceptions of students may also depend on their amount of familiarity with computer ethics-related concerns. The regulation of technology is far more complicated, controversial, and destructive than in the past due to the continual development of, reliance on and growth of cyber technology and advances within academic institutions. (Falconi, 2014:37) aver that “due to growing increase and reliance on cyber technology innovations and the Internet, certain measures have been adopted by many developing nations” (Aderibigbe, 2019:50).

Students may not be sufficiently informed about cyber ethics if their teachers are less informed too. A study by Milton *et al.* (2021) examined the understanding of cyber ethics that pre-teachers in Malta, Spain, and Norway possessed. The findings demonstrate that, compared to their Spanish counterparts, pre-service teachers in Malta and Norway demonstrated higher levels of knowledge and awareness regarding the application of copyright and respect for privacy standards. Norway and Malta were the countries with the greatest proportions of participants who indicated that they regularly evaluate the impact of posting materials online on their professional teaching careers. The country with the highest percentage of pre-service teachers who said they hardly ever considered the influence on their teaching career was Spain. The few examples apply to South Africa as well, where a teacher's unawareness of cyber ethical behaviour is likely to be low.

## **2.4. Forms/types of cyber ethics behaviour and violations revealed by students.**

In the fields of information technology and information science, cybersecurity is essential. Protecting data has become one of the most difficult tasks because of the advanced technologies that are used. According to Reddy and Reddy (2014:22), even the advanced technologies, such as cloud computing, mobile computing, e-commerce, and net banking, need a high level of security since they handle sensitive data about a person; therefore, security has become a top concern. According to Reddy and Reddy (2014:34), the word “cybercrime” refers to any legal activity that primarily commits theft and uses a computer to do it. Cybercrimes are crimes performed using computers, like network intrusions and the propagation of computer viruses, as well as computerised versions of other crimes, like stalking, bullying, identity theft, and terrorism, which have grown to be significant issues for people and the countries (Reddy and Reddy, 2014:58).

Peer pressure contributes to cybercrime. According to Festl and Quandt (2013:102), young adults, mainly in high schools, engage in cyberbullying to make themselves feel influential by exaggerating their social status and undermining that of their victim in their discussion group. Young adults can participate in cyberbullying anonymously, and it can take many forms, such as cyberstalking, harassment, deceit, denigration, imitation, exclusion, and flame (Moross, 2017). Social media has a significant impact on cybersecurity and contributes significantly to personal cyber threats (Reddy and Reddy, 2014:55). Social networking sites have become a popular place for hackers to access private information and steal crucial data, because the majority of people use them on a daily basis.

The following are cyber ethics violations.

### **2.4.1. Cyber crime**

The greatest danger currently facing all organisations worldwide is cybercrime. Additionally, not only businesses are at risk. People are also susceptible to hacker attacks. Jahankhani, Al-Nemrat and Hosseinian-Far (2014:12) state that the prevalence of cybercrime is rising, and the present technical approaches to combating it are

ineffective at halting this growth. This demonstrates the need for additional preventive measures to lower cybercrime. According to Maat (2009:59), cybercrime refers to all illicit services in which software, computer systems, communications systems, or data is the goal of the crime, as well as all known illegal actions or crimes that are actively perpetrated using computers, computer systems, or networking technologies. Wall (2007:34) contends that in order to define cybercrime, we must comprehend how information and communication technology have changed our society and the way we live. Through its distinct qualities, cyberspace offers new opportunities for criminals to perpetrate crimes. Cassim (2010:118) describes cybercrime as a type of crime carried out primarily via a laptop connected to the internet, with the computer being the victim or the perpetrator of the crime. While there is theft of computing devices, the objective perspective is that the computer is the aim of the crime. However, Leslie (2014:56) defines it as a legally sanctioned act that involves the use of automatic electronic equipment to execute mathematical or logical operations. For enforcement agencies, cybercrime is an inconvenience. This is due to the fact that tracing the perpetrator of these crimes is incredibly difficult and these miscreants can also simply erase their digital footprints (Thomas, 2018:06). In addition, the rate of cybercrime has risen at such an alarming rate that preventing a cybercrime has become nearly impossible.

#### **2.4.2 Cyberbullying**

According to Abaido (2020:407), modern communication is now almost entirely conducted online, which could promote undesirable or dangerous behaviours. One particularly disruptive or damaging behaviour is cyberbullying (Abaido, 2020:408). Bullycide has also become more common in many societies. According to Abaido (2020:407), cyberbullying is known as the problem of young people being bullied in many forms and then sometimes taking their own lives. According to recent research findings, individuals who use social media sites, especially young people, face major challenges due to cyberbullying and online harassment. Kowalski *et al.* (2014:1075), in a 2016 survey by the Cyberbullying Research Centre noted that, 33.8 percent of middle and high school pupils aged 13 to 17 had been victims of cyberbullying at some point. In addition, some of them had even committed suicide. According to Dixon (2019:19), on popular networks like Instagram and Snapchat, teenagers have been harassed, intimidated, or shamed.

Many high school students in different schools have experienced cyberbullying on social media platforms (Dixon, 2019:21).

Dixon (2019:20) further explains that women are much more likely than men to be both victims and perpetrators of cyberbullying; teens can be made to feel horrible about themselves by body shaming, rumours, and comments on social media posts. Teens can use social media to stay in touch with their friends and family. Moreover, some are captivated by the ability to upgrade their lives wherever they choose, for all to see, and when it comes to cyberbullying, teens are often unaware of the true consequences. According to Notar, Padgett and Roden (2013:133), many youths' perspectives of well-being, education, and peer relationships are impacted by cyberbullying. Harassment has long-term harmful effects on schooling, relationships, and the psychological and emotional well-being of young people who are victims; in some cases, the effects last into early adulthood (Notar, Padgett and Roden (2013:134). According to the National Crime Prevention Council's (2019), various research has identified significant elements that can assist schools in better grasping the nature of the cyberbullying epidemic and what they might do to support children. The overwhelming proportion of children affected by cyberbullying, as well as the substance of the communications, imply that cyberspace may be a graphic, scary, threatening, and overall disturbing virtual world with few regulations or socially acceptable conduct norms (Notar, Padgett and Roden 2013:134). Typical teen relationship concerns, such as break-up resentment, intolerance, and ganging up, are now being played out in a considerably more dangerous atmosphere (Notar, Padgett and Roden 2013:135). In an unsupervised context, students who often lack the moral compass or leadership qualities to govern themselves are increasingly interacting with classmates.

### **2.4.3. Identity theft**

Due to its widespread use, social media has surely become the talk of the town. This does not imply that all of these changes have been for the better, either. On the opposite end of the scale, social networking websites have helped by giving crooks and fraudsters new and inventive means to carry out their crimes. According to Irshad and Soomro (2018:43), social networking platforms have become a popular place for criminals to brag about their crimes, giving rise to "Performance Crimes". Identity thieves use low-tech

techniques to commit a variety of criminal offences under the umbrella of identity theft. Theft of an individual's identity can take many different forms, including financial, juvenile, and medical identity theft (Irshad and Soomro 2018:45).

In the UK, this sort of fraud is expanding the quickest (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014:159). The act of collecting private information about another person without that person's consent and utilising that information to perpetrate crime or fraud is known as identity theft (Jahankhani, Al-Nemrat and Hosseinian-Far, 2014:159). Due to the Internet, cybercriminals now have access to databases of vulnerable companies and can obtain this information. The All-Party Parliamentary Group claims that because of the expanding and changing techniques for obtaining and making use of personal information, identity fraud is a significant and growing problem both in the UK and internationally.

#### **2.4.4. Plagiarism**

Plagiarism is becoming more of an issue. According to Hanks (1979), plagiarism is defined as "the act of plagiarising," which implies "to appropriate (ideas, sections, etc.) from (another work or author)". Plagiarism is committed when someone copies somebody else's work and does not credit the writer. Plagiarism is frequently used to allude to the stealing of phrases or concepts that exceed what is considered common knowledge (Park, 2003:472). Academically dishonest research has frequently focused on the types of behaviours and behaviours that students are, likely to participate in, such as cheating in exams and tasks, falsifying data, plagiarism, improper use of funds, taking responsibility for work done by someone else, and manipulating academic staff (Raffetto, 1985 and Ferrell and Daniel, 1995). In high schools, students copy other learners' homework or assignments and present it as their own to the teachers, and if they don't get caught, they might continue doing it for the whole year. Kleinrock (2009) highlights the Internet's virtues, such as free information sharing and the exploitation of others' work, thoughts, and other digital works without acknowledgement or authorisation. The faster new inventions multiply, the less noticeable earlier ones become (Eisenstein, 1979:20).

### **2.4.5. Cyber piracy**

Perez and Choi (2007:168) point out that the illicit use or copying of intellectual or protected (electronic) material, such as music or computer downloads, is referred to as online piracy. Piracy is clearly unlawful and unethical. Nonetheless, some of today's firms, executives, and scholars that regard internet piracy just as a legal issue, or ignore it entirely as an inconvenience, risk missing the most significant advances throughout the Internet and information sectors (Perez and Choi, 2007:168). Whereas piracy-related copyright encroachment has driven businesses and social orders to require measures towards more noteworthy security and content protection, it was not recognised for its capacity to goad authentic businesses or financial esteem creation

Students tend to view or stream movies, YouTube videos and download music online without knowing the consequences or guidelines that need to be followed. Even scholars watch videos online. The ramifications of online piracy mostly on the media and software industries are both concerning and substantial (Perez and Choi, 2007:169). Piracy has become increasingly prevalent as the Internet has gone mainstream. Online piracy is a major source of worry and intrigue on the Internet and information sectors (Kaplan, 2005 and Lichtman, 2004). Online piracy has driven the development of lawful and creative companies, both directly and indirectly. In certain cases, such organisations have been technology firms adopting the convergence market to capitalise on new prospects (Perez and Choi, 2007:171). Some related studies to cyber piracy have been conducted by (Leonard *et al.* 2004) as they explore the determinants that affect piracy-related ethical conduct intentions. Kruger (2003) highlights the importance of introducing cyber-ethics with students.

## **2.5. Challenges in the efforts by high school students to act ethically when using cyber technologies.**

Most high schools in KwaZulu-Natal have no school libraries inside the school premises, making it difficult for students to act ethically when writing their assignments, and some are not even aware of unethical cyber behaviour. Furthermore, the shortage of school



libraries results to students rely more on cyberspace for information access. According to the Economic Commission for Africa (2014), cybercrime and a lack of regulation characterised increased cyber technology exposure in Africa, particularly in educational sectors. Bear (2014:72) discusses the difficulties in efforts made by students on college campuses to conduct themselves morally online, as well as the difficulties in schooling the consequences of cyber technology misuse. Many computers are contaminated with viruses and other harmful software, and cyber technology-related security issues such as cyber technology rules, legislation and other connected agencies are poorly understood.

There is a lack of adequate cyber ethics in high schools and a lack of incentives to incorporate cyber ethics into the curriculum (Rasmitadila *et al.*, 2020:92). The students who have little knowledge of cyber ethics are those doing business studies from Grade 10 to 12 concerning intellectual property. Other obstacles include a lack of qualified employees and teaching materials on cyber ethics, challenges with evaluating goals related to computer implications and ethics, as well as a shortage of qualified staff for cyber ethics teaching resources. Walczak *et al.* (2010:98) highlight inconsistencies in campus policies on academic dishonesty, curriculum overload, a lack of room for cyber ethics instruction, inadequate academic credentials among staff who are ideally equipped to inculcate cyber ethics, and a constrained view of technology. According to Stylianou *et al.* (2013:44), individuals and organisations are challenged with new issues arising from unethical information activities such as intrusions into personal privacy and intellectual theft, even beyond the undeniable benefits attributed to cyber technology.

According to Moskowitz (2017), existing research has demonstrated that due to the incredible increase in speed, space, and storage, as well as the continual development of cheap and economical cyber technology devices, the gathering, search for, storage of, access to, and sharing of images and information are now considerably faster and less expensive than ever before. Ethical issues with cyber technology are becoming more significant and concerning (Eldakak (2010), Davinson and Sillence (2010), Kavuk, Keser, and Teker, 2011). The present direction of study in information communication technology is reflected in cyber technology ethics (ICT). An examination of cyber technology ethics,

or cyber ethics, was carried out based on the more well-known subjects of computer and information ethics (Aderibigbe, Ocholla and Britz, 2021:390).

Researchers in Africa have studied the topic of cyber ethics and the obstacles that students face in trying to behave ethically in cyberspace. For example, Dadzie (2011:68) has found that within the setting of the academic environment in Ghana there are internal and external challenges in information ethics. Despite the fact that the threat of viruses and malware has existed virtually since the advent of computing, awareness of the security and sacredness of data on computer systems did not take hold until the Internet's spectacular rise. The introduction and subsequent acceptance of a new course in cyber ethics by academic staff at the universities, as well as a shortage of specialists and experts to teach the curriculum have already overloaded the majority of the schools' resources.

## **2.6. Appraisal of the chapter**

A research gap, also known as a literature gap, is a subject or problem that has not been thoroughly examined and answered in the literature (Moeini, 2014:22). According to Gowry (2014:67), a research gap is defined as an area in which missing or insufficient information prevents a conclusion for a question from being reached. Several publications have been reviewed, particularly those that deal with cyber ethics and misuse in various circumstances, particularly in academic activities.

In uMhlathuze Municipality, no study has been conducted about cyber ethical behaviour among high school students, while students do not recognise the unethical use of cyber technologies as they are exposed to social networks.

A recent study by Aderibigbe (2019:44) aimed at examining the phenomena of students' use of cyber technology that is either ethical or unethical at two universities in Africa. The study's findings showed that the majority of university participants in the sample were aware of online behaviour. The study suggested that universities should continue to offer orientation programs at the beginning of each academic year, especially for new students, on cyber ethics and cyber security knowledge so they can act properly in university cyberspace. It is also recommended that universities establish strict policies and corresponding penalties for cyber ethical violations or misconduct.

An in-depth study related to current research was produced by Chiang and Lee (2011), concerning the use of computers in an ethical manner. The research involved a poll of political science students in Taiwan, to examine their objectives for enhancing morality in the area of digital rights, including freedom of speech, association, equitable access to information, secrecy, and intellectual property protection. The findings revealed that more studies on cyber ethics in Taiwan and high schools are required, as respondents' attitudes, subjective norms, perceived behavioural control, and information ethics all significantly influence one's own perceptions of information ethics. However, in a study by Acilar and Aydemir (2010:2), students who use Internet technology are more likely to not show unethical use and behaviour trends.

The cited studies were aimed at university students who are older, better exposed and cognitively mature than high school students. Notably, studies focusing on school students in Africa seem to be insufficient. As a result, the current study will address this gap by filling in the evident gaps.

Aderibigbe (2019:20) compares the cyber ethical behaviour of undergraduate students at the University of Zululand and the Federal University of Agriculture in Nigeria. His study was focused on undergraduate students' online behaviours in terms of ethics as well as the relationships between students' demographic characteristics. The results demonstrated some differences in the association between respondents' demographic variables and their cyber ethical behaviour in South Africa and Nigeria. It confirms a fact: that participants from both Nigerian and South African universities are mostly aware of the different cyber ethical behaviours. This study focuses on the cyber ethical behaviour of university students. Chandarman and Van Neikerk (2017:134) wrote on students' understanding of cybersecurity at a private university. By examining the online behaviour of private higher learning students as well as their knowledge, self-perceptions of abilities, real skills and behaviours, and attitudes as they pertain to cybersecurity, their study sought to close the knowledge gap. It aimed at identifying the degree to which an intensive, targeted cybersecurity awareness education and training strategy is customised towards the audience, as opposed to a generic awareness campaign that is

relevant to all students. This study focuses on the cyberethical behaviour of university students.

Another study, by Chiang and Lee (2011), focused on the use of computers in an ethical manner by Taiwanese students studying politics, to analyse their goals of improving morality in the field of digital rights, such as freedom of speech, association, equal access to information, secrecy, and intellectual property protection. The findings revealed that respondents' attitudes, subjective norms, and perceived behavioural control have had a significant influence on personal information ethics judgments, indicating that additional study on cyber ethics in Taiwan and high schools is needed. However, in a study by Acilar and Aydemir (2010:3) students who use Internet technology are more likely to not show unethical use and behaviour trends.

Cilliers (2017) has written on evaluating information ethical issues among undergraduate students. The study reveals that the most common ethical issue that is faced by students is plagiarism and software piracy. The Internet makes computer science and information resources readily available; students believe that downloading movies or music from websites is reasonable behaviour. According to Akbulut *et al.* (2008:463), higher institutions are greatly worried that the Internet will encourage students to use information in an unethical or dishonest manner. Plagiarism, software piracy, fraud, fabrication, and information misuse are examples of unethical behaviour. Hence, the present study seeks to investigate the unethical behaviour of high school students in uMhlathuze municipal. The review of literature in the present study reveals that students in high school are not completely informed of their unethical cyber behaviour when using cyber technologies. Therefore, the study seeks to educate high school students about their unethical cyber behaviour in cyberspace.

Chatterjee, Sharker, and Valacich (2015) employ scenario-based academic research to elucidate the intricacies of numerous aspects impacting on young people's unethical cyber behaviour and use of cyber technology. The research's findings had numerous flaws, particularly a lack of sufficient qualitative data that may have revealed more nuances in the analysed variables' tensions and dialectic interactions. Another noticeable gap is that it appears that present theories used to study issues like student cyber-ethical

behaviour are lacking. As a result, the current study extended the findings to fill in a certain gap and employing a quantitative research method and investigating the phenomena of cyber ethics behaviour among high school students in the selected high schools in uMhlathuze Municipality.

## **2.7. Summary of Chapter two**

This chapter examined the literature related to the cyber ethical behaviour of high school students. The chapter discussed the theoretical framework that was employed in the study. Notably, the Theory of Planned Behaviour was considered to be the most suitable for this study and also discussed the research focuses which are the level of awareness of cyber ethical behaviour among the selected high schools in uMhlathuze Municipality, forms of cyber ethics behaviour revealed by the selected high school students, application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangenzwa High, Ongoye High and Empangeni High School and challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools. Different types of cyber ethics were discussed. The following chapter presents the methodologies and techniques used to carry out the full study.

## **CHAPTER 3: RESEARCH METHODOLOGY**

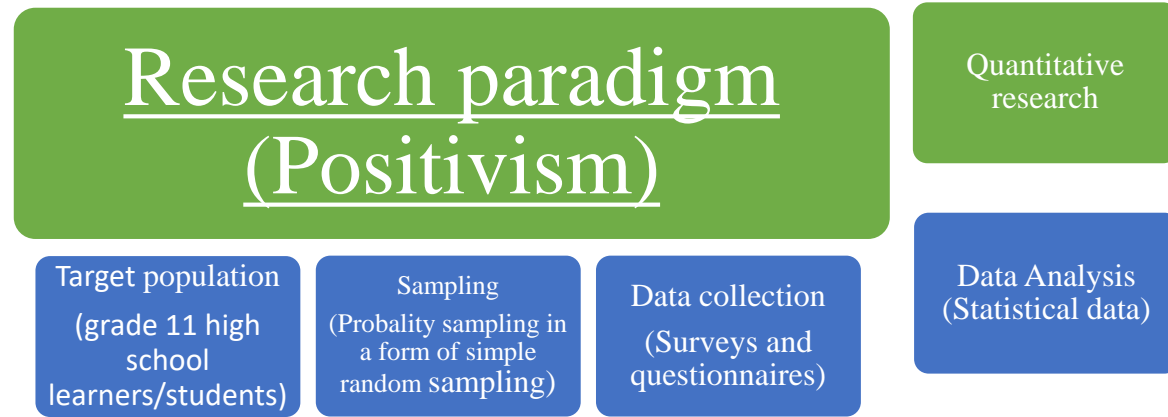
### **3.1. Introduction**

The findings from the subject literature were discussed in the two previous chapters. Chapter one provided the background to the importance of information ethics in high schools. Chapter one discussed the introduction and background of the study as well as a few facts about the approach utilised to conduct the entire study were mentioned. Greater insight into the definitions as well as an analysis of the literature was provided in chapter two. This chapter describes the methodology used to conduct the study on high school students' online conduct ethics in selected uMhlathuze Municipality schools. Some relevant studies (to mention a few such as Ajzen, 1991, Kortjan and von Solms, 2013, Aderibigbe, 2019, Ozer, Ugurlu and Beycioglu, 2011, Falcon, 2014 Oyewole, 2017) influenced the research methodology, strategies, and processes used in this study.

### **3.2. Research methodology**

The way a study is being conducted is referred to as its research methodology. Research methodology is defined and interpreted in various ways in subject specific literature. According to Struwig and Stead (2001;65), research methodology is a well-planned structured procedure, a method for gathering and analysing data used by researchers which is necessary to reach a solution to a problem. The research methodology consists of different elements. These include philosophical paradigms, methodologies/approaches, methods, sampling, data collection tools, data analysis, and other elements (Kumar, 1999; Kothari, 2004; Durrheim, and Painter, 2006; Williman, 2011; Creswell, 2014; Maree, 2016) are some of these factors. The following diagram represents the research methodology applied to this study.

# Research Methodology



## 3.2.1. Research paradigm

The term “research paradigm” has several definitions. For Hannes (2019:45) a research paradigm is known as a comprehensive cluster of substantive concepts, variables, and dilemmas, as well as the methodological techniques and instruments that go with them. Creswell and Creswell (2018:69) identify four common research paradigms in research, which are positivism, post-positivism, constructivism and transformative. A research paradigm is a group of convictions concerning key parts of reality that influence one's worldview (Maree, 2016:53). Maree (2016:53) further stated that the world is perceived according to paradigms as organising principles. Positivism was liberalised by post-positivism. Post-positivism is defined as a meta-theoretical position that evaluates and alters positivism and has affected speculations and practices across reasoning, sociologies, and different models of logical request (Prathapan, 2014:45). Honebein (1996:42) defines a constructivism paradigm as the way people see the world around them as a result of their “mind creation”. Participants have a voice thanks to transformative research, since it makes them more aware of issues or promotes reform that will make their lives better (Creswell and Creswell, 2018:57). According to Phillips and Burbules (2000:69), people's behaviour can be described in general by the gender conventions they've been subjected to as a result of their education, as well as their economic class, gender, and ethnicity. Therefore, the aim of a scholar is to identify the

rules that apply to human behaviour in the same way that scientists have established the rules that regulate the physical world. The positivist paradigm holds that there is only one truth, and that reality is unchangeable (Phillips and Burbules, 2000:69).

Positivism usually uses a quantitative approach in data collection and analysis in most studies (Creswell, 2014:11). Further it is explained that positivism is used to study and forecast behaviour that follows laws, a technique frequently employed in physical science, the natural sciences and to some extent in the social sciences, especially when a large number is involved. This study largely adopted a positivist paradigm to identify the factors that lead students to unethical behaviour when using cyber technologies. Quantitative survey research methodology was employed using the positivist paradigm. According to Phillips and Burbules (2000:69), real observations, measurable phenomena and objectives are the focus of positivism.

### **3.2.1.1 Positivism**

This study uses positivism and hence has adopted a quantitative research approach for gathering and analysing data. It is well known that optimism [positivism?] is geared to authentic, real, and genuine events that can be investigated and seen technically and experimentally, as well as explained by well-spoken lecturers and reasonable research and analysis methods (Aliyu *et al.*, 2014:82). A positivist researcher believes that the universe or world is governed by constant and unchangeable laws and principles underlying causality and events; there's an intricacy and complexity that may be conquered by relativism; and also, that objectivity, observation, and consistency are important (Aliyu *et al.*, 2014:84). Hence, positivist research technique (epistemological uniqueness) emphasises micro-level testing and experimentation in an experimental context, removing the complexity of the outside world. According to Kaboub, as cited by Aliyu *et al.* (2014:86) Auguste Comte's condemnation of metaphysics and assertion that only technical and scientific facts can reveal the reality regarding truth gave rise to the idea of positivism as a reality framework at the end of the nineteenth century.



### **3.3. Research approaches**

When conducting study, researchers choose one or more of three approaches, namely quantitative, qualitative, and mixed method research. Qualitative research involves collecting and analysing numerical data to understand concepts and opinions (Burnard *et al.*, 2008). Flick (2015:270) adds that qualitative research is not modelled on measurements and normally selects its participants purposively. The mixed research approach is for gathering, analysing, and combining quantitative and qualitative data within a single study at certain stages of the research process (Maree, 2016:169). Quantitative research is defined as an organized method of acquiring and analysing data from many sources, involving the use of computational and mathematical-based tools to determine the conclusions (International research, 2019:22). Park and Park (2016) add that quantitative research examines a large number of people, gives an overview of the area, and discovers patterns and inconsistencies.

In order to achieve a thorough grasp of the research problem, the researcher in this study used a quantitative research methodology based on the positivist paradigm from Ongoye Secondary, Dlangezwa High and Empangeni High School and their awareness of cyber ethical behaviour by polling. The ability to generalise information outcomes to the population from which they were acquired is a strength of the quantitative research approach (Bamberg, 2000:146).

#### **3.3.1. Quantitative research approach**

This approach was adopted in this study. The quantitative research approach, as used in this study, works with numbers and evaluates data using graphs, charts, and tables. Quantitative research is a systematic, objective procedure that employs statistical data from a subset of a sample to conclude the entire sample being examined (Struwig and Stead, 2001:104; Maree, 2016:162). Quantitative research has the benefit of allowing a large variety of studies to be studied in a short space of time (Flick, 2015:271). According to Flick (2015:271), when utilising this method, the findings are more generalised. Furthermore, despite the approach's advantages, there are still flaws to be addressed. According to Mthembu (2019:60), a quantitative research method may not always have the same depth of significance as a qualitative approach. According to Maree (2016:162),

surveys are utilised in most quantitative research studies, and the current study employed a questionnaire-based survey technique. In general, quantitative data gathering procedures are more organised than qualitative data collection approaches. Hence, structured questionnaires were used to gather data from Grade 11 learners in the selected high schools in uMhlathuze Municipality in this study. The next section discusses the research methods employed in this study.

### **3.4. Research design**

According to Kumar (2019:110) research design outlines how a study will produce responses to the research question; he also adds that the design aids in the production of reliable findings and conclusions. Kumar (2019:112) goes on to mention that the research design refers to the researchers' methods and procedures for collecting, analysing, and interpreting data. Data is gathered through a variety of methods, including observations, focus groups, content analysis, as well as questionnaires.

The survey study design was widely used to collect data via questionnaires, which is the most basic type of data collecting. It is possible to search and examine a variety of topics from a study population that uses this design and then validate the results to the sample population. Survey designs save time and money and are also accurate and easily maintained.

#### **3.4.1. Survey method**

In most research studies, including the current one, the survey approach employs questionnaires as data gathering tools. According to William, cited by Mthembu (2019:64), the most common and commonly utilised approach to gathering information from individuals is to conduct a survey. According to Pandey and Pandey (2015: 84), a survey method is "a procedure of acquiring quantitative information regarding the social element of a particular demographic structure and behaviours". According to Maree (2016:174), telephone conversations, emails, interviews, and questionnaires are all examples of ways to conduct surveys. Bryman (2012) defines survey research as a cross-sectional design in which data is mostly collected through self-completed questionnaires or structured interviews on one or more instances at a single moment in time to obtain a

corpus of quantitative or measurable information with regard to multiple variables, which are then carefully analysed for correlations among them.

The survey method's two primary characteristics are highlighted (Maree, 2016:174). The first characteristic is that samples are typically large. Second, a large number of variables are assessed, and a variety of hypotheses are evaluated. According to Pandey and Pandey (2015:87), the survey method has three advantages:

- The level of objectivity is very high.
- This strategy necessitates a strong collaboration between the researcher and the respondents.
- Cost and time savings are other important considerations while doing survey research.
- The survey method can be used anywhere.

The survey research became relevant to this study as it would be difficult to collect data from the entire school population who would have limited time to attend to the demands of a survey instrument, which is in line with the study's objectives of the cyber ethical behaviour of Grade 11 learners. Many studies have employed survey research as part of their studies. For instance, a study was done by Aderibigbe (2019) on the cyber ethical behaviour of undergraduate students at the University of Zululand, South Africa, and another at the Federal University of Agriculture, Abeokuta Nigeria. The adopted research methodology, the sort of data to be gathered, the sampling design, and the techniques of analysing the data collected all influenced the survey research design employed in this study.

### **3.5. Target population**

According to Maree (2016:176), a target population is the gathering of individuals or articles wherein an analyst chooses an example to break down and gather information. According to Creswell (2012: 381), the target population is the genuine rundown of testing units from which the sample is chosen. This study's intended audience were Grade 11 high school students from Dlangezwa High, Ongoye Secondary and Empangeni High School in uMhlathuze Municipality. Grade 11 students at the selected high schools were

chosen for this study because they are more exposed to technologies and smartphones. The study aimed at comparing the township high schools with the multi-cultural public schools that are situated into town. Hence, both schools are under government and students are exposed to cyber technologies as their preparing themselves for pre-matric. They use social networks to connect with others through Facebook, WhatsApp, Instagram and other networks. 480 students from the three chosen high schools made up the study's population.

### **3.6. Sampling**

According to Kumar (2019:177), "sampling is the act of picking a few samples from a larger group to serve as the foundation for evaluating or predicting the proportion of an uncertain set of information, circumstance, or outcome affecting the larger group." However, Gentles *et al.* (2015:28) define testing as the demonstration, cycle, or methods of selecting a subset of the population to determine the attributes of the overall population. Neuman (2011:102) explained that sampling is used to select a subset of people to be studied from the larger universe to which they belong, in one of several ways to be either representative or non-representative. Additionally, the sampling procedure is the way of selecting inclusion in a study, which is often done in a systematic manner (Kumar, 2014:65).

Thus, there are two forms of sampling known: probability sampling and non-probability sampling. Probability sampling refers to whether or not a unit in the population has an equal chance of being included in the sample (Pascoe, 2014:77). The probability of sampling methods includes cluster sampling, simple random sampling, stratified sampling, systematic sampling, and multi-phase seedling (Pascoe, 2014:77). Non-probability sampling is described as sampling that is utilised when determining who the entire population is or gaining access to the complete population is challenging (Pascoe, 2014:78). Finn *et al.* (2000) and Pascoe (2014) mentioned different types of non-probability such as quota sampling, snowball sampling and purposive sampling.

According to Cooper and Schindler (2008:54), when the objective is quite large, random sampling is frequently used. Hence, a purpose of a random sample is to reflect the entire

populace in an unbiased manner. People from the population who are regarded to be better positioned to provide the data collected can be chosen, while those who do not have the required data can be excluded (Cohen, Manion and Morrison, 2011).

The study used a probability sampling technique. The current study used simple random sampling by randomly selecting students in the population who are deemed to be better placed in providing relevant information as it strives to identify the most important factors that can lead to the unethical cyber behaviour of high school students. Meng (2013:531), simple random sampling is a fundamental type of sampling that is frequently used as a sampling approach in and of itself or as a foundation for more advanced sampling methods. Therefore, the simple random sampling principle states that every possible sample has the same chance of being chosen, although the concept of "possible sample" varies amongst sampling methods. With an equal chance of selection for each and every participant of the study population, it is the least controversial sampling technique. There were written numbers from 1 to 480 that were placed in two separate boxes. Individually students each took one number out of the first box without peeking inside. The learner was chosen for participation when the researcher selected a number at random from the second box and it matched the learner's number. Up until the sample size was reached, the researcher removed numbers at random. This means that each student had an equal probability of being chosen to participate in this research.

### **3.6.1. Sample size and sampling frame**

Gagne and Hancock's (2006:66) "sample size" is a group of people that is a subset of the whole population. However, Dudovskiy (2018:34) define the sample size as the number of persons from the evaluating outline who contribute to the critical information collection measure. The sample size was sufficient for this study and enabled the researcher to examining the unethical cyber behaviour of high school students in the three selected schools in uMhlathuze Municipality and gaining knowledge of the factors that led to such behaviour. The total number of individuals chosen from the population to take part in the study is known as a sample (McMillan and Schumacher, 1993: 693). 214 students make up the study's sample size. According to Krejcie and Morgan (1970), with a population of 480, the sample size is 214, per the sample size determination chart. Figures were written

in two boxes in this study; students selected a figure from the first box without checking within, and the researcher selected a number from the second box, also without checking. When the researcher's number resembled the learner's number, the learner was invited to participate in the study.

**Table 1: Study population**

School name	Actual class number	Sample size
Empangeni High Grade 11	169	75
Dlangezwa High Grade 11	191	85
Ongoye High Grade 11	120	54
Total	480	214

Below is the method used to sample the students.

Dlangezwa High grade 11:  $191/480 \times 214 = 85$

Ongoye High grade 11:  $120/480 \times 214 = 54$

Empangeni High grade 11:  $169/480 \times 214 = 75$

**N= 214**

### **3.7. Data collection instrument and procedures**

Data collecting instruments are the equipment that are used to collect data from the study's population (Gray, 2014:17). These tools are employed by the researcher to gather the research information. A research instrument is anything that acts as a method for gathering data for an investigation, similar to interviews or talks with guides, surveys, field journals, and notes on field perceptions and gathered data from optional notes (Kumar, 2014:380).

Roopa and Rani (2012:273) define a questionnaire as a series of questions about a single topic that are distributed to a specific group of people. This study adopted questionnaires to collect data from high school students. Questionnaires were distributed among Grade 11 students at the selected high schools in uMhlathuze Municipality. The researcher aimed at gaining a comprehensive knowledge of the research problem from Dlangezwa

High, Ongoye Secondary and Empangeni High School. Survey method was used in the form of a questionnaire to collect data from KwaDlangezwa High, Ongoye Secondary and Empangeni High School.

### **3.7.1. Questionnaires**

A questionnaire consists of a series of questions that is delivered in the very same manner to each and every respondent in a research project, whether in writing or orally (Flick, 2015:273). Questionnaires were distributed among Grade eleven high schools. The questionnaire instrument was deemed adequate for the current study because of its ability to cover large samples. According to Prathapan (2014:116), structured questionnaires, unstructured questionnaires, mixed questionnaires, and disguised-type questionnaires are the four types of questionnaires. A questionnaire is a good way to collect data, but it has a number of advantages and disadvantages (Maphoto, 2016:48).

Some of the advantages and disadvantages (Kumar, 2014:181 and Maree, 2010:57) are highlighted below.

- Despite the vast population, it is comparatively inexpensive.
- “Long-distance” participants could be approached.
- When participants are stumped by a question, the researcher will be right there to help.
- There are favourable chances of confidentiality since there is no one-on-one interaction, which increases anonymity.

Disadvantages include (Prathapan, 2014:117)

- The questionnaire might not even be returned by participants.
- Compiling questions and distributing questionnaires, as well as gathering them, takes a long time for a researcher.
- For those who are illiterate, they are irrelevant.
- Participants' subjectivity can influence how they mark their answers.

According to Kumar (2014: 181), a questionnaire has the following drawbacks:

- Self-selecting bias: Because questionnaires have a self-selection bias, it is not always the case that everyone who is given one returns it.
- The questionnaire has a chance of a low response rate: Since some participants might not even return questionnaires, the sampled population is impacted, and the results may not be generalizable to the entire group.

Even though a questionnaire has drawbacks, this study chose it because its benefits outweigh those drawbacks. The drawbacks of this technique won't have any bearing on the study, and the researcher was forced to ensure that the questionnaire's content was of a high standard by the various test administrators' comments. The teachers from the schools also ensured that all students return the questionnaires, even ones that were not completed. The questionnaires were distributed to the students and collected within the same day by the researcher.

### **3.8. Data analysis**

According to Kumar (2014:201), Data analysis is defined as "the process in which the investigator 'keeps digging into' the importance and communications in his or her findings and gains a knowledge of the subtleties, organisation, and analytical possibilities." Data analysis is made up of several linked procedures that aid in the summarisation and evaluation of obtained data to respond to the research questions (Kothari, 2004). The quantitative data gathered using a structured questionnaire was analysed using descriptive statistics and the Statistical Package for the Social Sciences (SPSS) since it enabled simple modification of statistical data analysis and interpretation of quantitative study results (Pallant, 2013:101). Pickard (2007:278) points out that SPSS can make it simple for a researcher to extract useful information from data. Findings were presented through graphs and charts. Taking into consideration the omissions and mistakes that had been made throughout the investigation, the researcher analysed the data obtained to construct meaning.

### **3.9. Reliability and validity of the instrument**

Unreliable and non-validated research is invalid. According to Gray (2014:22), validity is a metric that determines how well a measuring device detects what it purports to measure. For Maree (2010:25), when an instrument is used at different times or on various kinds of



people in the same population, it produces consistent results. The accuracy of the study's method or procedures is referred to as its reliability (Maphoto, 2016:49). However, a study that is dependable but not valid is pointless. The significance of reliability and validity in the findings was established in this study by gathering data utilising questionnaires among Grade 11 students from the three selected schools in uMhlathuze Municipality.

The researcher carried out a pilot investigation in this study on Grade 11 students at Qhakaza High School in order to improve the questionnaire's reliability and validity. According to In (2017:602), pilot research is carried out on a lesser scale than the primary or full-scale investigation, which is another distinctive design element. To put it another way, the pilot study is crucial for increasing the efficiency and quality of the main study. Therefore, the school was picked because it had similarities with the study's chosen schools. Pre-testing helped the research since it allowed the researcher to correct grammatical and question-construction errors based on the results and interpretation of the pilot study. To take part in the pilot study, 10 volunteers from the class were chosen at random. The information gathered from the students during the pilot project was utilised to determine how long it took to complete the questionnaire. The pilot study assisted the researcher in determining if the students would be able to finish the questionnaire in the allowed 15 minutes, as the researcher had predicted. The responses supplied by the Qhakaza High School pupils also assisted the researcher in determining if the students understood the questions. The researcher was able to establish whether the language and vocabulary used in the questionnaire were understandable to students in those grade levels. If a substantial number of the questionnaires had all of the questions completed, it was apparent that students understood the questions. If students had left many questions unanswered because they were difficult for them to understand, the researcher would have concluded that specific questions needed to be reconstructed. Furthermore, the researcher is certain that the results would be the same or identical if the study were replicated. Participants were promised complete anonymity, allowing them to express themselves freely without fear of being identified.

### 3.9. Ethical considerations

Ethics is highly important in research. Prathapan (2014:234) considers ethics to be a set of standards that researchers adhere to in their academic endeavours. Prathapan (2014: 234) argues that a researcher bears a great share of responsibility for society's direction. Every research project has an ethical component; the goal is to conduct research responsibly without harming the participants. Mertens (2012:19) stresses the importance of adhering to the behavioural standards and recommendations established by the institutions that participate in all academic research. Proper data collection and processing includes things like appropriate study methodology, the right interpretation of the data, accurate reporting, no data fabrication, and no criminal conduct. As a result, the researcher adhered to ethical standards. After finishing the research proposal, the methodology, and content of this study were given to the university ethics committee. The University of Zululand Research Committee and the Department of Information Studies both authorised the study and gave a letter of permission to conduct research. The ethical clearance letter is evidence that the University has approved the proposed research project (attached as Appendix 1) as it was shown to the three selected high schools.

The research instruments and the ethical clearance letter were submitted to the Department of Education in KwaZulu-Natal to request the Department's approval letter to conduct the study from the schools in the jurisdiction of the KwaZulu-Natal Province (attached as Appendix 2) prior to collecting data. The schools were then provided with the informed consent letter along with the letter from the Department of Education to request authority to operate the research at their school (attached as Appendix 3). The study must closely abide by the ethical considerations when conducting study on children or minors. Therefore, a parents' consent form (Attached as Appendix 4) was also given to them in order for parents to grant permission for their children to engage. According to the "Age Admission Policy for Public Schools" (cited by the Department of Education, 2008:13), students between the ages of 14 and 18 are eligible for enrolling at secondary schools. It was vital to obtain parental permission because, according to the law, high school students are considered to be minors. The students were given the consent letters that they were to send to their parents in order to request permission for their children to

engage in this study. This author returned to the school the following day to collect the consent forms, at which point those students whose parents had given permission for them to participate might do so. A “gatekeeper’s” letter (attached as Appendix 5) as approval that of the research to be conducted at the schools was obtained. This investigation secured the participants in the examination, by guaranteeing that confidentiality is kept and that respondents are kept anonymous. Along these lines, the examination maintained the necessary ethical standards when leading the hands-on work and the arrangement and rules archive given by the University of Zululand that diagrams moral practices were considered over when directing this exploration. The researcher guaranteed that members participating are protected.

### **3.10. Methodological limitations**

Limitations are factors occurring within a study over which the researcher has no control. During data collection the researcher faced some few challenges, which are as follows:

- The majority of the data was gathered during sport time because the teachers couldn't find time for a researcher to gather it during free periods.
- Some participants did not return the parents' consent form on time, which resulted in the researcher having to come back and collect them the following day.
- Requesting a letter of authorisation from the Department of Education under uMhlathuze circuit took some time and it was a long process, but the researcher remained calm until it was received.
- The gathering of research data and the creation of exam questions happened both at the exact same time; as a result, the researcher had to postpone data collection.
- Since there are not enough workshops at the University of Zululand that teach one how to analyse data using the SPSS analysis, the researcher asked one of the lecturers in the Department to help out with the basics of SPSS.

### **3.11. Summary of the chapter**

This chapter describes the research methodology used in the study. It covered a wide range of topics, including research paradigms, research methods, study populations, sampling techniques, data collection instruments, data processing, pilot studies, validity and reliability, and research ethical issues, as well as information on mapping the

research methodology (see Appendix 7), informed by a positivist research paradigm. It was determined that the study employed a quantitative research approach. The survey method was used in the form of questionnaires to collect data from the Grade 11 students in the selected schools. The sample frame was then discussed and elaborated on how students were sampled. The pilot study's findings assisted in improving the data collection tool's reliability and clarity. All ethical protocols were observed and followed during data collection even though the researcher faced some challenges when collecting data. The study's findings are presented in the next chapter.

## **Chapter 4: Data Analysis and Presentation of Findings**

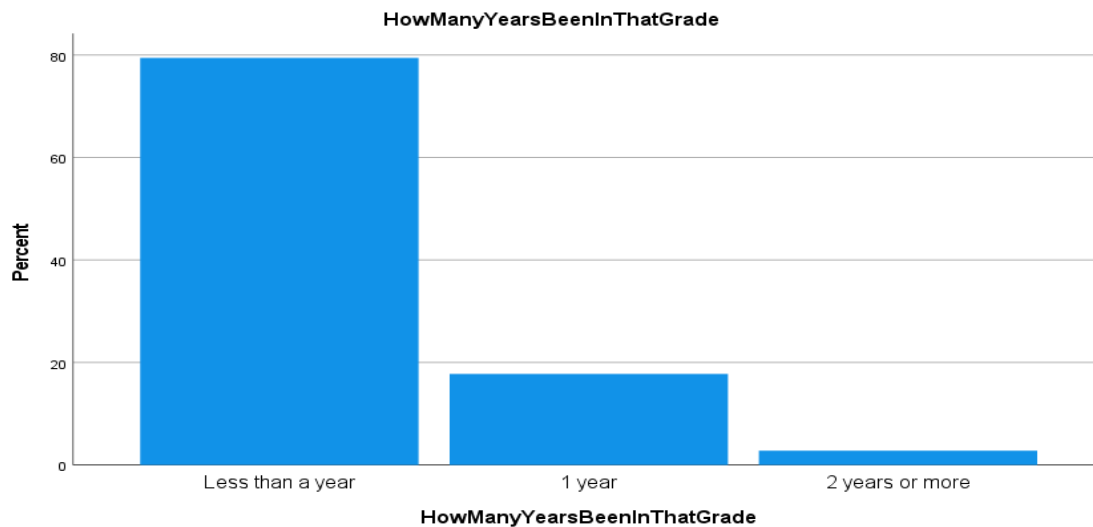
### **4.1. Introduction**

The previous chapter explained the methodology, techniques and strategies that were used to conduct the entire study. This chapter discusses the research findings, which were derived from questionnaires distributed to Grade 11 students of Dlangezwa High, Ongoye High as well as Empangeni High School in order to understand their cyber ethical behaviour when using the Internet. These three schools are situated in uMhlathuze Municipality. In order to allow for logical interpretations, the presentation of the analysis and findings is sequential, following the order of the research objectives and tools. To evaluate quantitative data, the researcher distributed and collected 214 questionnaires from the Grade 11 students in the studied environment and employed the Statistical Package for the Social Sciences (SPSS) to analyse data that was collected from the students. The data is analysed through tables, graphs and pie charts. From the three selected high schools in uMhlathuze, Grade 11 students were selected using simple random sampling. The subsequent research questions were developed and studied in order to acquire a better understanding and a larger picture of the subject under consideration.

1. What is the level of awareness about cyber ethical behaviour among the selected high schools in uMhlathuze Municipality?
2. What are the forms of cyber ethics behaviour revealed by the selected high school students?
3. How does the Theory of Planned Behaviour influence high school students' behavioural intentions in Dlangezwa High, Ongoye High and Empangeni High School?
4. What are the challenges to the efforts by high school students to act ethically when using the Internet and computers at three selected high schools?

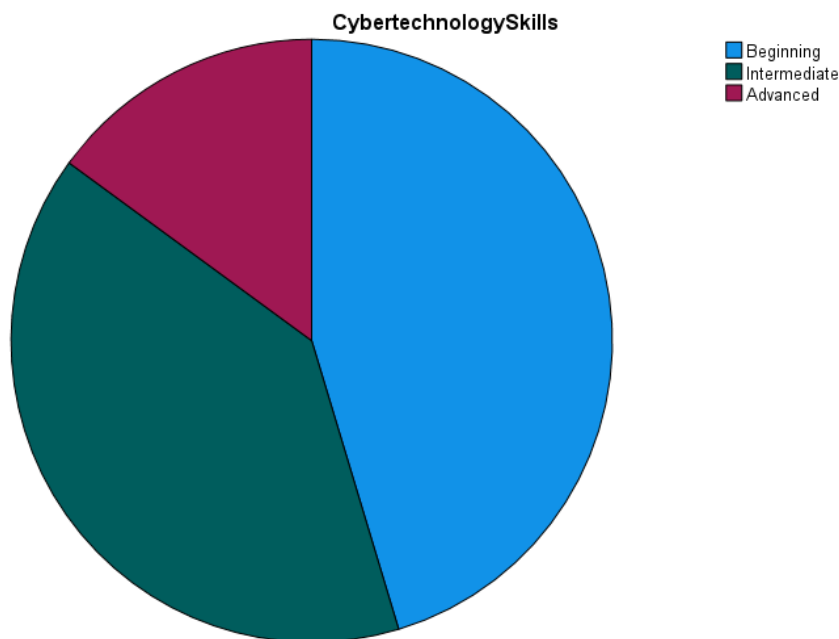
## 4.2. Profiles of the participants

Most of the students came from Dlangezwa, Empangeni and Ongoye high schools respectively. Most participants were females between the ages of 17-20 followed by 14-16 males. The majority had spent less than one year in the grade (**Figure 2**).



**Figure 2: Years spent in a grade**

Coming to cyber technology skills, the majority were beginners (**Figure 3**)

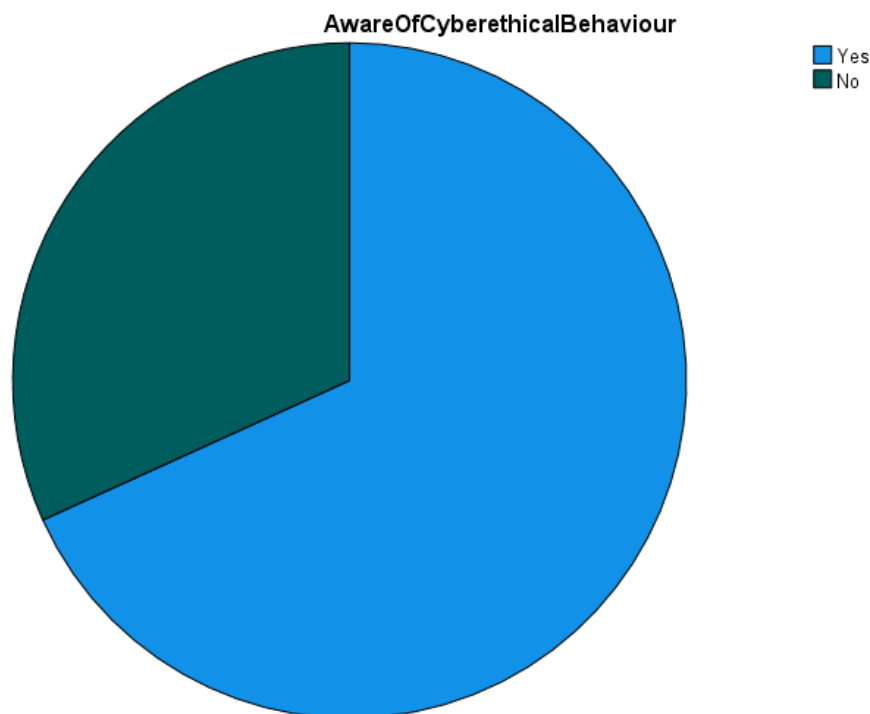


**Figure 3: Cyber technology skills**

## **Research question 1: Awareness of cyberethical behaviour**

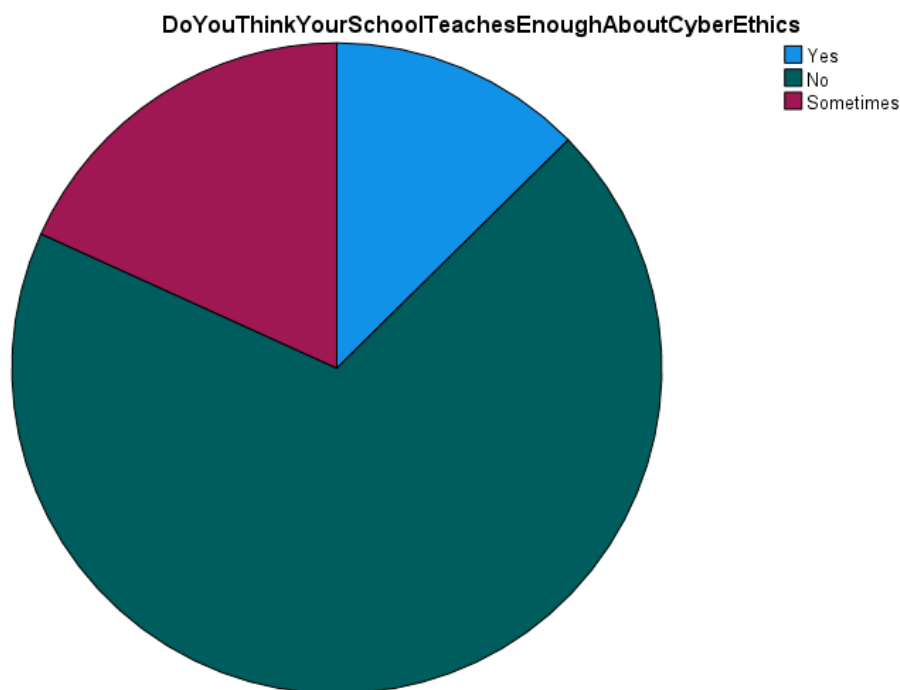
### **4.3. Awareness of cyberethical behaviour**

It was important to know if the respondents were aware of their cyberethical behaviour. To determine that, students were asked if they are aware of cyberethical behaviour. Most of the respondents 146 (68.2%) were aware of their cyber ethical behaviour. Less than half 68 (31,8%) of the respondents showed less awareness (**Figure 4**).



**Figure 4: Awareness of cyberethical behaviour**

Regarding awareness by teaching cyber ethics, Students were asked if their school teaches enough about cyber ethics. The majority said No with a few saying Yes, while others did not respond to this question (**Figure 5**).



**Figure 5: Teaching of cyber ethics**

They were then asked why do they think so, the responses were as presented in Table 2

**Table 2: Awareness of cyber ethics**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	The school doesn't teach us about cyber ethical behaviour	58	27.1	27.1	54.7
	I have never heard of this word before	56	26.1	26.1	52.3
	Our teachers don't care whether or not we're bullied.	27	12.6	12.6	72.0
	There are only two teachers who teach Life Orientation	13	6.1	6.1	96.3
	They never mentioned it	9	4.2	4.2	58.9
	It's because we are not taught enough about this and it's quite a serious issue that needs to be addressed	3	1.4	1.4	76.3



Because I don't know anything about it	1	.5	.5	72.4
Because not everyone in the school knows about cyber ethics and its concept	1	.5	.5	72.9
Because they are also not that much educated about it	1	.5	.5	73.4
Because they don't want us to be fully aware of it and pay attention to it	1	.5	.5	73.8
Because it's the first-time hearing about it	1	.5	.5	74.3
Even they don't know	1	.5	.5	74.8
I am not exposed to some cyberbullying	1	.5	.5	75.2
I don't take the subject that deals with cyber ethical behaviour	1	.5	.5	75.7
I have never been taught about this	1	.5	.5	76.2
I have no idea	1	.5	.5	76.6
I have not heard this word before	1	.5	.5	77.1
In this school, we are against bullying	1	.5	.5	77.6
Insufficient resources	1	.5	.5	78.0
It is because they do not want us to take pictures or videos at school	1	.5	.5	78.5
It is not in the curriculum	1	.5	.5	79.0
It's because we are not taught enough about this and it's quite a serious issue that needs to be addressed	3	1.4	1.4	80.4
It's not part of the curriculum	1	.5	.5	80.8
Limited resources	1	.5	.5	81.3
Occasionally, the school calls people to address the learners about cyber ethics	2	.9	.9	82.2

Our school teaches us about this	3	1.4	1.4	83.6
So, we can use these ethics and skills outside of school as the world is slowly moving into a technical and digital world	2	.9	.9	84.6
Some give information about it but not very clear	2	.9	.9	85.5
The school does teach us about cyber ethics	1	.5	.5	86.0
The school doesn't teach us about cyber ethics	1	.5	.5	86.4
The school has more than enough technological resources that are used for educational purposes	1	.5	.5	86.9
The school has not taught us about this	1	.5	.5	87.4
The school has provided us with adequate resources for educational purposes	1	.5	.5	87.9
The school teaches basic knowledge on cyber ethics but not enough to be effective; the majority focus on cyberbullying unless you take subjects like CAT	1	.5	.5	88.3
The teachers do not teach us about cyber ethics	1	.5	.5	88.8
The teachers might be overloaded with the school curriculum	1	.5	.5	89.3
Multiple subjects provide useful skills and tasks based on technology and the Internet	2	.9	.9	90.2

There are very much overloaded with different work	1	.5	.5	96.7
They do teach us.	1	.5	.5	97.2
They focus on abuse rather than cyberbullying	1	.5	.5	97.7
They sometimes teach us about cyber ethics	1	.5	.5	98.1
They touch on the topic but do not go into details	1	.5	.5	98.6
We are not taught about it	1	.5	.5	99.1
We learn about cyber ethics but not frequently	1	.5	.5	99.5
We usually come across cyber ethics lecturing if one of our peers has been victimised	1	.5	.5	100.0
Total	214	100.0	100.0	

There were many reasons that were shared by the students, but most of them were saying they had never had the words cyber ethics or cyberethical behaviour mentioned in their school. What appears in Table 2 shows the urgent need for cyber ethics education in schools.

## **Research question 2: types of cyberethical behaviour**

### **4.4. Types of cyberethical behaviour**

It is possible to be aware of what one does not know. The respondents were asked to identify cyberethical behaviour that they are aware of from a controlled list in Table 3.

**Table 3: Types of cyber ethical behaviour known to students**

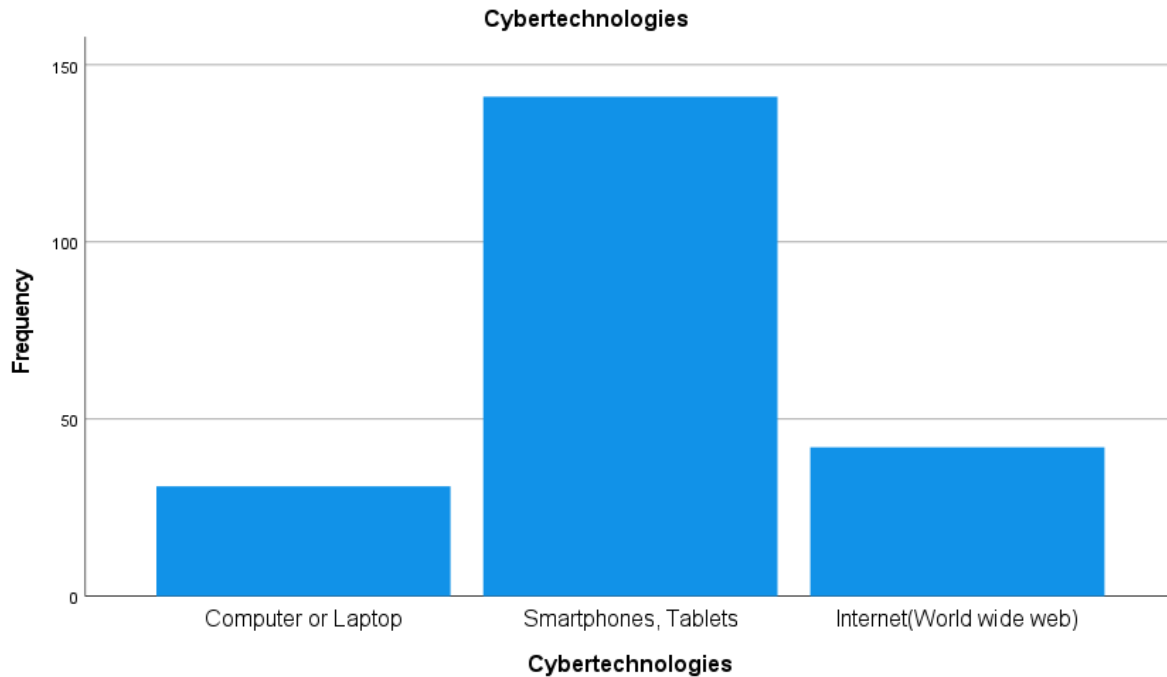
NO	Cyber ethics behaviour	Frequency	%
1.	Cyberbullying	122	57
2.	Using another user's password	35	16.4
3.	Dissemination of fake news	18	8.4

4.	Cybersquatting	8	3.7
5.	Cyber piracy (Software piracy: music and film downloading)	7	3.3
6.	Cyberstalking	7	3.3
7.	Hacking/ carding/cracking	5	2.5
8.	Cybercrime	3	1.4
9.	Cybersex (Online porn and pornography)	3	1.4
10.	Cyber fraud	3	1.4
11.	Cyber vandalism	2	.9
12.	Plagiarism	1	.5
13.	Identity theft	0	0
14.	Privacy violation	0	0
15.	Copyright violation	0	0

It is noted that respondents are aware of more than one cyber ethical behaviour, although it seems they are experiencing cyberbullying (57%) more than any other type of cyber ethical behaviour. Cyberbullying is quite common in schools.

When it came to cyber technology, the respondents were asked to tick cyber technologies to indicate those they use or experience. The most popular were smartphones and tablets (**Figure 5**)

N=214



**Figure 6: Cyber technologies in use**

The figure above indicates that 31 (14,5%) of the respondents were using or aware of computers or laptops, whereas 141 (69.9%) of the respondents were using cellphones and tablets to access the Internet and social media. Forty-two (42;19.6%) of the respondents indicated that they are aware of the Internet. The results suggest that the learners use cell phones more than other cyber technologies.

**Scale: 1= Strongly Agree, 2= Agree, 3= Neutral, 4=Disagree, 5=Strongly disagree (N = 214)**

The respondents were then asked to indicate their level of agreement with the statements that are applicable to elements of cyber technology behaviour awareness as indicated in Table 4.

**Table 4: The level of awareness of cyber technology**

	<b>SA</b>	<b>%</b>	<b>A</b>	<b>%</b>	<b>N</b>	<b>%</b>	<b>D</b>	<b>%</b>	<b>SD</b>	<b>%</b>
I am aware of the issues and repercussions of cyber technology behaviour as a student	79	36.9	74	34.6	34	15.9	17	7.9	10	4.7
Cyber ethics behaviour is affected by skills and knowledge of cyber technology	71	33.2	69	32.2	53	24.8	10	4.7	11	5.1
I sometimes read about problems of unethical use of cyber technology	44	20.6	75	35	59	27.6	20	9.3	16	7.5
Cyber behaviour is influenced by the ability to make decisions based on prior knowledge.	42	19.6	85	39.7	52	24.3	27	12.6	8	3.7
I seek guidance on the use of cyber technology in various forums on the Internet.	30	14	54	25.2	66	30.8	35	16.4	29	13.6

The above Table (4) indicates that 75 (35%) of the respondents agreed that they sometimes read about the unethical use of cyber technologies, whereas 54 (25.2%) of the respondents agreed that they seek guidance on the use of cyber technology. Seven-one (71;33.2%) of the respondents strongly agreed that cyber ethical behaviour is affected by skills and knowledge that people have about cyber technology. Other respondents (85;39.7%) agreed that cyber behaviour is influenced by the capability to make judgments based on prior knowledge, with 79 (36.9%) of respondents strongly agreeing that they are aware of the issues and repercussions of cyber technology behaviour as students. The results suggest that cyber technology behaviour awareness among high school learners is limited.

### **Research question 3: Influence of attitude, subjective norm, and perceived behavioural control on cyber ethical behavioural intention**

#### **4.5. Attitude towards cyber technology behaviour**

**N=214**

**Table 5: Attitude toward cyber technology behaviour**

NO	Attitude towards cyber technology behaviour	Yes	%	No	%
1.	It is not essential to report instances of cyber ethical violations.	60	28	154	72
2.	Learners regard incidents of cyber ethical violation as commendable behaviour.	125	58.4	89	41.6
3.	It's tempting to engage in unethical cyber technology behaviour.	118	55.1	96	44.9
4.	I will urge another learner to engage in the improper use of cybertechnology.	89	41.6	125	58.4

The above Table indicates from the 1<sup>st</sup> statement that 60 (28%) of the respondents said it is not essential to report cyberethical violations whereas 154 (72%) of the respondents disagreed with the statement, which shows that more than half of the respondents' attitudes towards the cyberethical behaviour is positive. In the second statement, 125 (58.4%) of the respondents indicated that they regard incidents of cyberethical violation as commendable behaviour and 89(41.6%) of the respondents disagreed with the statement which shows that more than half of the learners are violating cyber technologies. In the third statement, (118;55.1%) of the respondents agreed with the statement, and 96 (44.9%) disagreed with the above statement, which indicated that most learners find it tempting to engage in unethical cyber technology behaviour. In the last statement, 89 (41.6%) of the respondents agreed with the statement and 125 (58.4%) disagreed with the statement, which means the learners have little knowledge or awareness of cyberethical behaviour.

##### **4.5.1. Subjective norms**

The respondents were given four statements that were about subjective norms.

**N=214**

**Table 6: Subjective norms**

NO	Influence of Subjective Norm on the Use of Cyber technology	Yes	%	No	%
1.	My classmates prefer carrying out this behaviour.	126	58.9	88	41.1
2.	My principal will want me to carry out the action.	62	29	152	71
3.	My religious community will back me up if I indulge cyber technology behaviour.	83	38.8	131	61.2
4.	My family will be delighted to witness me indulge in unethical cyber technology behaviour.	92	43	122	57

The above Table indicates that 126(58.9%) of the respondents in the first statement agreed with the statement, and 88(41.1%) of the respondents disagreed with the given statement, which shows that more than half of the learners are carrying out unethical use of the cyber ethical behaviour at school or home. In the second statement, 62 (29%) of the respondents agreed with the statement, whereas 152 (71%) of the learners disagreed with the given statement. Therefore, learners do not believe that their principal would allow them to carry out this behaviour. In the last statement, 92(43%) of the respondents agreed with the given statement, and 122 (57%) disagreed.

#### **4.5.2 Perceived behaviour**

The respondents were given four statements that were related to the perceived behaviour.

**Table 7: Perceived behaviour**

NO	Influence of PBC on Unauthorized Use of Cyber technology	Yes	%	No	%
1.	As a learner, it is quite easy for me to engage in unethical cyber behaviour	114	53.3	100	46.7
2.	It would be relatively easy for learners at this high school to exploit cyber technology unethically.	152	71	62	29



3.	I could easily carry out unethical use of cyber technology and not get caught.	81	37.9	133	62.1
4.	My cyber technology behaviour is neither controlled nor prevented by the school's cyber technology policy.	124	57.9	90	42.1

The above table indicates statements that are related to the perceived behaviour. One hundred and fourteen (114;53.3%) of the respondents agreed with the given statement and 100 (46.7%) of the respondents disagreed with the statement; this means half of the learners (53.3) find it easy to engage in unethical cyber behaviour. In the second statement, 152 (71%) of the respondents agreed with the statement and 62 (29%) of the respondents disagreed. Hence, high school learners find it easy to exploit cyber technology unethically. In the third statement, 81 (37.9%) agreed with the statement whereas 133 (62.1) of the respondents did not agree. Therefore, this shows that some learners find it hard to commit the unethical use of cyber technology. This could be caused by not all of them having cellphones or the Internet. One hundred and twenty-four (124;57.9%) of the respondents agreed with the statement and 90 (42.1%) of the respondents disagreed. This means that the learners believe that their cyber ethical behaviour is not controlled by their school or parents, since they already indicated in Figure 5 that their schools don't teach much about this topic.

### 4.5.3 Influence of Behavioural Intention towards Cyber technology Behaviour

**N=214**

**Table 8: Influence of Behavioural Intention towards Cyber technology Behaviour**

NO	Influence of BI towards Cyber technology Acts	Yes	%	No	%
1.	Friends and peers have an impact on a person's cyber technology behaviour, both good and bad.	205	95.8	9	4.2
2.	The religious background of the student may influence some cyberethical goals and behaviour.	179	83.6	34	16.3

3.	The school's morale has little bearing on learners' cyber technology behaviour.	133	62.1	81	37.9
----	---	-----	------	----	------

The above Table indicates that 205 (95.8%) of the respondents believe that their friends and peers have an impact on their cyber technology behaviour, and 9(4.2%) of the respondents disagreed with the statement. One hundred and seventy-nine (179;83.6%) of the respondents also agreed with the statement that their religious background may influence some cyber ethical behaviour, whereas 34 (16.3%) did not agree with the statement. In the last statement, 133 (62.1%) of the respondents agreed with the given statement and 81 (37.9%) disagreed with the statement. By looking at the Table it means that schools still need to teach learners about cyber ethical behaviour and the proper use of cyber technology.

#### **Research question 4: Challenges of cyber ethical behaviour among high school students**

#### **4.6 Challenges of cyber ethical behaviour among high school students**

The respondents were given the following statements that relate to the challenges of cyber ethical behaviour among high school students. The researcher wanted to see if they really face challenges as high school learners.

N=214

**Table 9: Challenges of Cyber ethical behaviour among high school students**

NO	Challenges of cyber ethical behaviour among high school students	Yes	%	No	%
1.	Inappropriate use of cyber technology due to a lack of cyber morality and ethical behaviour	179	83.6	35	16.4
2.	There is a lack of policy guidelines on how to utilise and behave appropriately online.	181	84.6	33	15.4
3.	Appropriate understanding of cyber behaviour is extremely limited.	142	66.4	72	33.6
4.	Inadequate security measures to ensure that cyber ethics policy is followed.	136	63.6	78	36.4
5.	Breach of network integrity and confidentiality	142	66.4	72	33.6

The first statement in the Table above indicates that 179 (83,6%) of the respondents agreed with the given challenge statement and 35 (16.4) of the respondents disagreed with the statement. By looking at the percentages the learners encounter challenges of cyber ethical behaviour as they tend to use cyber technology inappropriately due to the lack of cyber morality. One hundred and eighty-one (181;84.6%) of the respondents agreed that there is a lack of policy guidelines on how to use and behave appropriately online, whereas 33 (15.4%) of the respondents did not agree with the given statement. One hundred and forty-two (142;66.4%) of the respondents agreed with the statement and 72 (33.6%) of the respondents did not agree with the given statement; by looking at the numbers a high number of 142 of the respondents believe that the knowledge or understanding of cyber technology is extremely limited. One hundred and thirty-six (136;63.6%) of the respondents agreed with the statement and 78 (36.4) of the learners did not agree. In the last statement, 142 (66.4%) of the respondents agreed with the statement, and 72 (33.6%) did not agree with the given statement. Therefore, by looking at the percentages of all the given statements, they all have a high number on the Yes part, which means learners do face challenges of cyber ethical behaviour, it could be at school or at home. The inappropriate use of cyber behaviour is a great issue among learners.

## **4.5 Summary**

This chapter gave the entire set of questionnaire results. Pie charts, tables, and graphs were used to illustrate the data on the cyber ethical behaviour of high school students in the selected schools in uMhlathuze Municipality. The study's research questions, which included promoting cyber ethics awareness, identifying the different types of cyber ethical behaviour among students, examining the impact of the Theory of Planned Behaviour on students' cyber ethical behaviour, and discussing the study's findings in relation to cyber ethics behaviour all guided the discussion. Data were collected from the three high schools, namely Dlangezwa High, Ongoye High, and Empangeni High School. The Statistical Package for Social Sciences (SPSS) version 28 was used to analyse quantitative data. The findings aided in identifying the kind of challenges that high school students confront. Regarding the awareness of cyber ethics in schools (see Table 2) learners in Grade 11 listed their different views pertaining to cyber ethics.

The most relevant conclusions drawn from the findings are as follows: the students did not seem to be aware of the schools' ethical cyber-ethics training requirements (see Figure 3). The schools from the sample environment are not teaching enough about cyber ethics (see Figure 5). Secondly, amongst the several types of cyber ethics behaviour, cyberbullying, using another user's password and dissemination of fake news ranked the highest amongst them all, and most students agreed that cyber ethical behaviour is affected by skills and the awareness of how to use cyber technologies. Thirdly, the use of cyber technologies by high school students is very high, yet they do not know the principles and policies guiding how to use it without violating the rights of their peers (see Figure 6). The results are discussed further in the following chapter.

# CHAPTER 5: DISCUSSIONS OF FINDINGS

## 5.1 Introduction

This chapter reflects on the key findings that arose from the data interpretation and analysis (Chapter 4) to highlight how the findings enrich the body of knowledge and theories used in this study. After reflecting on the objective and application of research on interpreting, a range of concepts, models, and multidisciplinary techniques are used as a starting point for a reflection on the course's identification as a scientific discipline. The study aimed to investigate unethical online behaviour among high school students in three selected schools in uMhlathuze Municipality, as well as the factors that contribute to such behaviour. The study used the Theory of Planned Behaviour and addressed the research topics stated in Chapter One. The following research topics were developed and studied in order to acquire a better understanding and a larger picture of the subject under consideration.

1. What is the level of awareness of cyber ethical behaviour among the selected high schools in uMhlathuze Municipality?
2. What are the forms of cyber ethics behaviour revealed by the selected high school students?
3. How does the Theory of Planned Behaviour influence high school students' behavioural intention in Dlangezwa High, Ongoye High and Empangeni High School?
4. What are the challenges to the efforts by high school students to act ethically when using the Internet and computers at three selected high schools?

The demographics of the respondents, such as their gender, age, race group, grade, name of the school, level of study and cyber technology skills are reported in the previous chapter (see 4.2 in Chapter 4).

## **5.2. Profiles of the participants**

This portion included the demographics of the respondents, such as their gender, age, race group, grade, name of the school, level of study and cyber technology skills (see 4.2 in Chapter 4).

## **5.3. What is the level of awareness about cyber ethical behaviour among students at the selected high schools in uMhlathuze Municipality?**

There are different definitions of awareness. Awareness is thought to be a precursor to the construction of attitudes and the eventual formulation of intentions prior to behaviour (Aderibigbe, 2019). Determining respondents' awareness and understanding of the concerns related to cyber ethics misuse that are highlighted in the survey instrument is the foundation for eliciting respondents' thoughts on the degree of their awareness of cyber ethics misuse behaviour (Ajzen *et al.*, 2011:105). Children these days spend more time than any previous generation addicted to their gadgets and technology in the age of screens. Undoubtedly, the Internet has provided a wealth of options for today's students to learn and develop their imaginations. The Internet's limitless knowledge also fosters creativity and fosters an environment that may help a child's intellect grow in more ways than ever before. According to Giaever *et al.* (2016), the perceived complexity of these domains makes the legal facets of cyber ethics, copyright and privacy, for example, less accessible in classroom education. The potential gap between pre-service teachers' stated beliefs and their awareness and behaviours must be recognised. The Maltese curriculum for schools specifically mentions "respecting the use of the Internet responsibly" in addition to "making informed decisions about privacy, taking responsibility for their actions, recognising intellectual property, complying with the terms and conditions of the systems they use, and respecting the rights and feelings of others" (Directorate for Quality and Standards in Education [DQSE], 2015:46). Similarly, the Norwegian curriculum defines cyber ethics as the competence to follow privacy regulations and use media responsibly, including methods for avoiding unwelcome online interactions, reflecting ethically, and determining their own position in society and on the internet.

In their model of the moral decision-making procedure for software piracy, based on generic ethical decision-making theory, Wagner and Sanders include ethical awareness as one of the often-mentioned models of software piracy (Wagner and Sanders, 2001). Aderibigbe (2019:190), emphasised that it can be concluded that if a person has a favourable awareness of cyber ethics misuse behaviour, there is a chance the person will engage in such behaviour. As stated by Moor (1985:268), computer science is a field that is always evolving. Therefore, all users of cyber technology must be conscious of how their behaviour affects other people. To be able to recognise and respond to the new problems that cyber technology will offer, they must increase and maintain their awareness. Ethical dilemmas in cyberspace have been linked to a lack of cyber ethical awareness (Kuan, Idrus, Mutton, 2015). This raises the issue of how to encourage this understanding and how to equip current and future high school students to take on this responsibility.

The results of the questionnaire reveal that the three high schools in the study have relatively high levels of awareness of cyber ethics. One hundred and forty-six (146;68,2%) of the students said they are aware of cyber ethics (see Figure 4) but when they were asked about their awareness by teaching cyber ethics, 84,3% said No, with a few saying Yes with others not responding to this question (Figure 5). This suggests an inadequate knowledge of cyber ethics in schools. In a new era with the proliferation of social media and Internet technologies for daily use by students, such an omission can be catastrophic to teaching and learning in schools. The creation and expansion of awareness and education, for a comprehensive grasp of the ramifications of cyber ethics abuse behaviour, should be a priority for every school seeking to secure its network and cyberspace. Therefore, a focus on education and training activities should be made for students who will begin their careers in higher institutions as cyber professionals so that they can investigate in-depth both the fundamental aspects of cyberspace and acquire hands-on experience on the tools and techniques of the area (Schweitzer, Gibson, Bibighaus and Boleng, 2009).

The present study's findings on cyber ethics misbehaviour of high school students in the selected schools in uMhlathuze Municipality are also supported by studies that were

completed by the Council of the European Union (2015) and other developed countries on the awareness of cyber ethics misuse behaviour. The European Union's decision-making body is more aware of cybercrime as a result of a project carried out by the data protection and cybercrime division to ensure a comprehensive response to cybercrime and other cyber offenses involving the use of cyber technology and electronic evidence. The project's significant accomplishments include enhancing cooperation, introducing legal reforms, raising awareness, and establishing a network.

Studies in the past have shown that students still have a complicated relationship with cyber technology. While they understand its value, students still need ethical guidelines for how they use it in their lives or on university campuses (Dahlstrom, Eden and Bichsel, 2014). It is essential to emphasize from the preceding that students' increased awareness of the phenomenon of cyber ethics misuse behaviour may not translate into an understanding of the ethical implications of their own behaviour. This is because more students in the 21<sup>st</sup> century own mobile devices than ever before, and that their use of these devices in class has become a distraction.

#### **5.4. What are the forms/types of cyber ethics behaviour revealed by the selected high school students?**

There are many types of cyber ethical behaviour that are reported in the literature, as reflected in Chapter two and recently discussed in a related study (Aderibigbe and Ocholla, 2020). The survey questionnaires that were submitted and collected from the high school students revealed that students experience considerable cyberbullying in schools. Cyberbullying, using another user's password and disseminating fake news led the pack in the three selected schools in uMhlathuze Municipality. This challenges schools to teach learners about the dangers of misuses of these types of behaviour. For example, raising awareness and implementing programs that teach aspects of these types of cyber ethics can reduce the high percentage occurrence of these types.

As a result, the findings of this study imply that there are modest variances, mostly in results obtained from the three high schools in uMhlathuze Municipality on the types of



violations that may be attributable to the lack of control of network access, where student users typically have a less favourable attitude toward cyber ethics misuse behaviour. According to Khalil and Seleim (2012), users in colleges and universities have engaged in a variety of cyber ethics abuse behaviours. Aderibigbe (2019), Harris and Furnell (2012) and Oyewole (2017), wrote about the misuse of cyber technologies by students. Harris and Furnell (2012) further emphasised that the utilisation of cyber technologies in the academic setting is insecure due to students' actions. Tavani (2013:65), argues that by using these technologies, schools will be able to give their students an education that satisfies current industrial demands and teaches cutting-edge technical skills. They will also enable life-long learning to progress from being just an idea to becoming a possibility. Lau and Yuen (2014) contend that young adults, who are sometimes referred to as "digital natives," have better access to cyber technology and are more information consumers than previous generations, but they lack discernment and the ability to make the appropriate choices when presented with ethical dilemmas. This approach to comprehending the multiple roles in a bullying situation has been critiqued as entirely individualistic, classifying, behavioural, and stigmatising. It also has a propensity to overlook the school's institutional setting, the interpersonal processes of those engaged, and the ways in which historically based, and societally established structures of inequality contribute to bullying in schools (Bansel *et al.*, 2009; Davies, 2011; Duncan, 2013; Horton, 2011; Kofoed and Sondergaard, 2009).

The findings from studies by Ibrahim (2016) and Ebenezer (2014) on youth cyber ethics misuse behaviour in Nigeria were also supported by the results. For instance, studies by Chatterjee, Valacich, and Sarker (2012) and Supavai (2014) discovered persistent evidence of chosen students' disregard for, or ignorance of ethical conduct or implications came up with results that followed a similar trend. Yan (2012) asserts that cyber behaviour, also known as human behaviour in cyberspace, is only a combination of cyberspace and human behaviour. Real-world behaviour and cyber behaviour are two categories of human behaviour that are distinct from one another but related. The phrase "cyber behaviour" describes how users behave when utilising various cyber technologies for diverse reasons. Therefore, it is the application of new technological devices, particularly in cyberspace.

It is still unknown whether students are aware of this legal sanction for unethical cyber behaviour. This might help explain why people engage in these vices without fear of punishment. However, the prevalence of cyber ethics abuse among undergraduate students may indicate that students and young adults in general lack a strong ethical foundation. Norms are rarely governed by laws and principles (Wolfe *et al.*, 2008). A study by lyadat, lyadat, Ashour, and Khasawneh (2012) found that in order to avoid the legal ramifications of user violations, ethical violations connected to breaking into a computer system for illicit purposes and other misuse behaviour in institutions should be taken very seriously.

It is crucial to keep in mind that the current data depends on how much access students have to computers, laptops, tablets, and the Internet. It was evident that students use smartphones more than laptops to connect to the technology world. This simply means there are variations in the forms of cyber ethics infractions engaged in by the high school students. Due to its low cost and wide availability, students are more prone to commit crimes and act unethically online. Peer pressure and other social forces are additional potential explanations for the online infractions.

### **5.5. How does the Theory of Planned Behaviour influence high school students' behavioural intention in Dlangezwa High, Ongoye High and Empangeni High School?**

The theory of Planned Behaviour is important and widely used in cyber ethical research, as reported in a recent study (see Aderibigbe, Ocholla and Britz, 2021). According to the theory of planned behaviour, among the categories of causes are people's beliefs concerning behavioural control, subjective norms, and attitudes toward the activity. Descriptive and inferential statistics were used to examine the impact of the Theory of Planned Behaviour (TPB) on the cyber ethical behaviour of the high school participants in this study. The core concept of the Theory of Planned Behaviour is that attitudes, subjective norms, and PBC all work together to establish behavioural intention and predict actual behaviour (Ajzen, 1991). The study's findings proved that the three basic theories

of the theory: attitude, subjective norms, and perceived behavioural control, are true, considerably and uniquely influenced high school students' desire to violate cyber ethics, which in turn was significantly connected with their actual behaviour (see Table 5 in Chapter 4). The elements of the Theory of Planned Behaviour have a considerable influence on students' behavioural intention and, as a result, their cyber ethical behaviour. The findings revealed that attitudes, subjective standards, and perceived behavioural control all had a significant impact on students' cyber ethical behaviour in high schools. The findings show that 95.8% of participants believe that their peers have an influence on their cyber technology behaviour. This alone shows that high school students are easily influenced by people around them. Regarding perceived control behaviour, half of the learners (53.3) find it easy to engage in unethical cyber behaviour. Hence, high school learners find it easy to exploit cyber technology unethically.

A study by Ibrahim (2016) found that rather than being affected by significant others, cyber ethics misuse behaviour is more frequently caused by or impacted by structural or socioeconomic reasons. Hence, Russo *et al.* (2015), reported that only direct measures of attitude and PBC strongly predicted intention, according to path analysis. The intention was not predicted by the subjective norm. The best indicator of intention was PBC. The findings support the TPB as a viable theory that might be used to account for users' propensity to engage in unethical online behaviour. This research confirms previous findings: that attitude, subjective norms, and perceived behavioural control all influence intention and behaviour. According to the findings of Peace, Galletta, and Thong (2003), user attitudes, subjective norms, and perceived behavioural control all have a significant impact on online behaviour. This study's findings are consistent with those of Stone *et al.* (2010), Ajzen (1991), and Aderibigbe (2019), who discovered subjective norm to be a key factor influencing students' inclinations to engage in various unethical cyber activities.

According to Aliyu *et al.* (2010), perceptions and attitudes concerning cyber ethics behaviour have a substantial impact on how people utilize cyber technology. They demonstrate how background elements like general opinions, personality qualities, moral beliefs, and a sense of right and wrong all impact on students' views on cyber ethical behaviour. Other research (Leonard and Cronan 2005; Kreie and Cronan 2000) have

highlighted perceived personal gain, personal views, and qualities (i.e., religious ideals). Negative moral judgment as well as the economic and hedonistic benefits have been cited as reasons for the public's attitude toward cyber ethics (Cesareo and Pastore 2014). According to Chiang and Lee (2011), female students studying at a Chinese university place great value on using cyber technology effectively, especially when it comes to upholding laws, personal privacy, and intellectual property rights. Because there are few ethical and legal restraints, it is safe to claim that many undergraduate students have unfavourable sentiments about cyber technology usage

In addition, Venkatesh *et al.* (2003) noted that when examining how people use technology, the Theory of Planned Behaviour has frequently been chosen as a prominent approach. Additionally, this supported the theories propounded by Russo *et al.* (2015), Cronan and Douglas (2006), Chatterjee *et al.* (2015), Chan and Wong (2015) and Chai, Wang and Xu (2020) that attitudes and perceived behavioural control affect high school students' cyber ethical behaviour. The works of Al-Rafee and Cronan (2006), Cronan and Douglas (2006), Cronan and Al-Rafee (2008), Chatterjee *et al.* (2015), and Chan and Wong (2015) reported that a crucial antecedent of cyber ethics misuse behaviour is the subjective norm. The study's findings back up the claims made by Ajzen (1991), Snyder, Jones and Bianco (2005), and Aliyu *et al.* (2010) and Russo *et al.* (2015) that a person's attitude toward particular behaviour influences the individual's participation; in this case, it is cyber ethical behaviour.

Additionally, this research backs up the findings of Ajzen (1991; 2006), who found that people have a strong propensity to engage in behaviour when they have a reasonable amount of genuine control over it. The ease of access and the students' demonstrated proficiency in using cyber technology, as evidenced by their experience, were used to perceive behavioural control. The availability of smartphones to be used by learners pushes them to use the Internet and social networks.

## **5.6. What are the challenges to the efforts by high school students to act ethically when using the Internet and computers at three selected high schools?**

There are many challenges attributed to cyber ethical behaviour in the subject literature (see 2.5). According to Stylianou *et al.* (2013:44), individuals and organisations are challenged with new issues arising from unethical information activities such as intrusions of personal privacy and intellectual theft, even beyond the undeniable benefits attributed to cyber technology. The high school students revealed that there is inappropriate use of cyber technology due to a lack of cyber morality and ethical behaviour, and some reported that appropriate understanding of cyber behaviour is extremely limited. The students are not aware of the cyber ethical behaviour when they are using the Internet. Hence, not many studies have been conducted in high schools regarding cyber ethical behaviour. Inadequate security measures to enforce compliance with cyber ethics policy, a shortage of adequate alignment and education about the consequences of ethical violations, an overburdened teaching and learning syllabus, a dispute between authorship and access to information, a lack of cyber morality and ethical conduct in the use of cyber technology, management bureaucratic processes, and breach of confidentiality are some of the challenges. Other obstacles to undergraduate students' efforts to behave morally online include poor understanding of computer literacy and cyber technology, insufficient understanding of the ethical aspects of cyber technology, and a lack of training resources (Haughton *et al.*, 2013). During the 21<sup>st</sup> century students are able to use cyber technologies for their personal matters and also for their educational purposes. Consequently, concerns about cyber ethics behaviours have been generated by limitless access to cyberspace. For instance, the rise in intellectual property crimes, such as software piracy and imitation of works of art in literature, music, movies, and videos, has grown concerning (Rujoiu and Rujoiu, 2014).

Understanding security, privacy concerns, and the significant negative effects of cyber technology on cyberspace is particularly crucial. The security of data, information, and computer networks can be jeopardised by several internal and external threats on a global scale, so everyone should be concerned about computer ethics. According to Gunarto (2003), a growing number of ethical issues resulting from the detrimental effects of IT on

our global society must be addressed by global law enforcement in addition to technical solutions like encryption, digital IDs, and firewall techniques. Gunarto (2003) further explains that to ensure that this worldwide knowledge is used for our future benefit and applications, governments of every nation, public policymakers, computer experts, organisations, and individual citizens must all take an interest in the issue and contribute. Despite the fact that ethical norms restrict the use of such technology to prevent ethical violations in so many schools, research suggests that students lack a grasp of ethical issues, awareness, and cyber technology use. Due to students' ignorance, judgements on their use and duties in the area of cyber ethics are made without prior knowledge (Moor, 1985). Ocholla (2009) found results that followed a pattern that was remarkably similar to his own, including issues with poor laws and enforcement, inadequate information, a shortage of curriculum space, sub-par professional practice, and issues related to the use of cyber technologies.

Numerous research studies on young individuals' use of cyber technology in a university setting makes use of moral theoretical notions. Others (Capurro, 2008) provide broad ethical guidelines for the use of cyber technology. Some scholars (Vallor, 2010; Calvani *et al.* 2012; Plaisance, 2013) have argued that the moral aspects of cyber technology should be considered. Some of the literature claimed that, like previous technical breakthroughs and innovations throughout human history, cyber technology has both positive and negative consequences on society and often creates moral and ethical dilemmas (Stahl, Eden and Jirotko, 2013 and Von Schomberg, 2012). The impact of information and communication technology (ICT) and its moral application on African communities have not been extensively written about (Capurro, 2008). There aren't many studies on cyber ethics in Africa, especially in high schools, and the study of recent patterns of unethical behaviour is still in its infancy here. As a result, the majority of African research on cyber ethics adopts Western philosophical traditions as their points of reference.

The findings of this study also shed new light on previous findings by the National Cyber Security Alliance (2009), which found that financial constraints, time constraints, bureaucracy, and an overburdened syllabus were the barriers preventing students from

acting in a morally proper manner. Similarly, Walczak *et al.* (2010) also draw attention to the following issues: inadequate training and incentives for integrating cyber ethics into the curriculum, inconsistent campus policies on academic dishonesty, incomplete curricula, inadequate cyber ethics education, a shortage of academics with the necessary credentials to teach cyber ethics, and a constrained view of cyber technology. Some, on the other hand, have argued that separating ethical challenges will result in a lack of connections and a poor reflection of the entry of moral considerations and computing into the domain. This viewpoint was also expressed in a paper published by De Melo and De Sousa (2017), who expressed concern about the educational system's unresolved concerns as a result of a lack of integrated courses in cyber ethics education for undergraduate engineering students.

Indicated by the findings, an intervention on guiding education students on how to behave in cyberspace is really recommended. This backs up research from the University of North Carolina (2014), that found students encounter a variety of cyber ethical issues brought on by individual and environmental factors that make it difficult to behave morally in cyberspace. According to Moor (1985), the majority of the user-generated cyber ethical dilemmas centre on concerns with privacy, accuracy, property, and accessibility. DiScala and Weeks' (2013;46) research supports this: given that the establishment of Internet laws reduces uncertainties regarding security in the use of cyber technology, the prevalence of these cyber ethical misconducts is unexpected.

The study identifies an absence of cyber ethics education in high schools and a shortage of specialists and experts to lead the course. This is due to the fact that teachers are not paying much attention to this topic because they believe it doesn't affect them and the children, whereas it should be taught in high schools so that as students get into the higher institution, they are already aware of these unethical acts in cyberspace. Other evident issues in a study by Aderibigbe and Ocholla (2020) include an absence of sufficient education for cyber ethics educators, a lack of cyber morality, and unethical behaviour when utilising cyber technology, among others.

## **5.7. Summary**

As expected, like any study conducted in the world, it was found that high school students are not being taught enough at schools about cyber ethics. Figure 4 and Table 2 in Chapter 4 indicate the need of cyber ethics education in schools as some learners indicated that they have never heard the word cyber ethics in their school. This chapter examined the findings of the study in view of the theoretical framework, a literature review, and the findings of a previous study of a similar nature. The chapter tried to clarify any potential consistency or inconsistency between the earlier studies and the current situation. This chapter went into details by clarifying the research questions of the study. The chapter also examined the level of awareness of cyber ethics among high school students at the three selected schools in uMhlathuze Municipality. The behaviour differs from one to another in the selected schools. This chapter also discussed the forms/ types of cyber ethics behaviour revealed by selected Grade 11 students. The formulation also considers how the Theory of Planned Behaviour (TPB) affects the individuals under study's behaviour in terms of cyber ethics. The three main dimensions in the applied theory, namely as attitude, subjective norms, and perceived behavioural control, exercised some importance and impact on cyber ethics behaviour in the high schools under investigation. This supported the theory's applicability to the investigation of cyber ethical behaviour. The challenges that high school students experience in trying to act ethically when utilising the Internet and cyber technology were discussed. Section 4.6 in Chapter 4 shows by looking at the percentages that the learners do encounter challenges of cyber ethical behaviour as they tend to use cyber technology inappropriately due to the lack of cyber morality. There are more challenges faced by Grade 11 students that are revealed in Table 9. The next chapter contains the study's summary, conclusions, and recommendations.



## **CHAPTER 6: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS**

### **6.1. Introduction**

The previous chapter went into detail about the study's findings. This chapter summarises, concludes and suggests recommendations for this study based on the findings on the cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality. The conclusions were drawn using survey designs and recommendations for future research were suggested based on those findings. The following objectives that were established have been addressed by the study's conclusions and recommendations:

1. To determine the level of awareness of cyber ethical behaviour among the selected high schools in uMhlathuze Municipality.
2. To identify the forms of cyber ethics behaviour revealed by the selected high school students.
3. To demonstrate the application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangenzwa High, Ongoye High and Empangeni High School.
4. To determine the challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools.

### **6.2. Summary of findings by research objectives**

In accordance with the study's objectives and research questions, the findings of the study are explained in this portion of the chapter.

#### **6.2.1 To determine the level of awareness of cyberethical behaviour among selected high schools in uMhlathuze Municipality.**

- What is the level of awareness of cyberethical behaviour among selected high schools in uMhlathuze Municipality?

Falconi (2014) emphasised that the regulation of technology is now far more complicated, controversial, and disruptive than it was in the past, due to the continual development,

reliance on, and growth of cyber technology and advances within academic institutions (Falconi 2014). To combat the growing reliance on cyber technology and the related online behaviour, developing countries have begun awareness and education programmes. Numerous studies have demonstrated that awareness is a key factor in determining cyber ethical behaviour. According to Galvez and Guzman (2009:4), awareness influences behaviour. As a result, they found that "the greater the cyber ethics awareness, the greater the practicing of cyber ethics behaviour." According to Kortjan and von Solms (2013:289), education and understanding of cyber ethics are necessary for implementing ethics in cyberspace. However, they noted that educational institutions in South Africa provide instruction and understanding of moral cyber behaviour.

The information from the questionnaire collected from the Grade 11 students showed the high level of awareness of cyber ethics even though when they were asked about the teaching of cyber ethics in schools, they reported that there is no teaching of cyber ethics in schools. This alone showed that teachers are not putting much effort into ensuring that the learners are aware of this cyber behaviour before they even leave the secondary level for tertiary studies. The study noted that students have beginning skills on cyber technology skills. Hence, they use these technologies every single day for their personal matters even for their educational activities. It is also noted that students make use more of smartphone or tablets to access the Internet than computers.

### **6.2.2 To identify the forms of cyber ethics behaviour revealed by the selected high school students.**

- What are the forms of cyber ethics behaviour revealed by the selected high school students?

Cyber technology's outstanding and remarkable qualities, which have provided pupils with a ground-breaking means of thought and worldwide knowledge, come with new difficulties (Aderibigbe, 2019:213). Puspita and Rohedi (2018) note that the modernisation and sophistication of Internet technologies have both positive and undesirable consequences for users, particularly among students.

The study has noted that cyberbullying (57%), using another user's password (16.4%) and disseminating of fake news (8.4%) are the mostly common types of cyber behaviour

being experienced by the students in the studied high schools. The use of cyber technology, particularly smart gadgets and the cyberspace, has also become an important part of students' everyday routines, whether they attend high schools or colleges. The availability of these cyber technologies has resulted in an increase in the gravity of ethical issues among students.

### **6.2.3 To demonstrate the application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangezwa High, Ongoye High and Empangeni High School.**

- How does the Theory of Planned Behaviour influence high school students' behavioural intention in Dlangezwa High, Ongoye High and Empangeni High School?

According to the significance levels of the data, the three components (attitude, subjective norms, and perceived behavioural control) were each statistically significant in determining students' cyber ethical behaviour. According to Aliyu *et al.* (2010), perception of and attitude to cyber ethics behaviour have a big impact on how people utilise cyber technology. They demonstrate how background elements like general opinions, personality traits, moral ideals, and a feeling of right and wrong influence students' perspectives regarding cyber ethics behaviour. Perceived power and control belief, or the propensity to act in a specific way while being inspired by a view of the anticipated success of the executed activity, are two more characteristics that influence perceived control. When students believed that their friends were utilising technology in various unethical ways, the use of cyber technology was found to be high (McCabe and Trevio, 1997).

According to Aderibigbe (2019,215), cyber ethics intentions are influenced by subjective norms, which are significant factors. Therefore, it is reasonable to believe that group norms, such as family, friends, or teachers, whom kids view as important in their daily lives, influence their development of cyber ethical misuse behaviour. In other words, these close friends and family members could serve as a substitute for the public influence needed to create either a favourable or negative intent toward students' cyber ethical misuse behaviour. Therefore, this study advises focusing on these significant group

norms when developing a plan for a campaign or a convincing argument against cyber ethics misuse behaviour.

#### **6.2.4 To determine the challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools.**

- What are the challenges to the efforts by high school students to act ethically when using the internet and computers at three selected high schools?

Researchers from Africa have also published their results on the difficulties pupils encounter when attempting to act morally online. Stylianou *et al.* (2013) emphasised that although there are certain advantages to cyber technology, consumers and organisations now face new issues brought on by unethical information practices, such as invasions of privacy and theft of intellectual property. In this study Grade 11 students reported that there is inappropriate use of cyber technology due to the lack of cyber morality, teachers are not teaching enough about cyber ethics and the use of cyber technologies and lack of policy guidelines. Some students reported that they have never heard the term cyber ethics before. This alone shows that there is still a need for a major intervention in schools by teachers and the Department of Education to visit and teach students about this. Similarly, Aderibigbe and Ocholla (2020) noticed, among other things that, there is a lack of cyber morality and ethical behaviour in the use of technology, inadequate training for teaching cyber ethics, etc.

### **6.3. Conclusions**

The most relevant conclusions derived from the findings are as follows: students did not seem to be aware of the schools' ethical cyber-ethics training requirements, but they are mostly aware of cyber ethics behaviour indications in the study. The schools from the sample environment are not teaching enough about cyber ethics. Secondly, amongst the several types of cyber ethics behaviour, cyberbullying, using another user's password and dissemination of fake news ranked at a high percentage amongst them all and most students agreed that cyber ethical behaviour is affected by skills and awareness of how to use cyber technologies.

One of the major conclusions of the Theory of Planned Behaviour (TPB) is used in this study to incorporate all of the components that express cyber-behavioural patterns and cyber ethical awareness. The theory describes how high school students are influenced when utilising cyber technology and involves subjective norms, behavioural control, and attitudes. The theory's direct and ongoing link with other ethical theories, and the practical consideration that goes along with students' immoral behaviour using the Internet, despite the theory's strengths and faults and criticism for those weaknesses, are crucial.

At least two limitations apply to the report's conclusions. First of all, the study was strictly directed to the Grade 11 students at the selected schools in uMhlathuze Municipality. Second, all the respondents to the study were asked to complete the questionnaire in English, which was their second or third language. The majority of the words or phrases might have been read differently or incorrectly. Some of the questions' contexts and nuances may not have been properly appreciated, which could have affected the study's conclusion. Lastly, because situational elements were not considered in the study, it is unclear why some moral ideologies had no effect on participants' ethical judgments and behavioural intentions in the ethical scenarios.

#### **6.4. Theoretical implication**

The research is important in the context of the selected high schools in uMhlathuze Municipality because it informed students regarding cyber ethical behaviour and other types of cyber ethics. If there is a sense that the knowledge is being used in lawful, upright ways, it can be deemed a public good. This could aid in extending the Theory of Planned Behaviour's use in cyber ethics research. Overall, the findings of this study demonstrate the relevance of the Theory of Planned Behaviour in comprehending the many types of behaviour associated with cyber technology users.

This study's findings imply that the overall model and data are well-matched. The Theory of Planned Behaviour can be used to foresee a wide range of cyber-related behaviour patterns. The theory's ability to predict behaviour is aided by the three predictor constructs developed by Ajzen: attitude toward behaviour, subjective norms, and perceived behavioural control. The significant impact of perceived behavioural control in the setting of this investigation was an intriguing theoretical discovery.

Not many studies have been conducted on high school students regarding cyber ethics. Therefore, this study seeks to raise awareness of cyber ethics among high school students. The study discloses that individuals' intentions toward a certain cyber behaviour are highly influenced by their attitudes toward cyber ethics issues, subjective norms, and perceived behavioural control.

## **6.5. Contribution of the study**

Concerning the study's contributions, the findings were significant because they demonstrated that the study was only undertaken with high school students in the three selected schools within uMhlathuze Municipality with the goal of examining the unethical cyber behaviour among high school students in the three selected schools within uMhlathuze Municipality and gaining knowledge of the factors that lead to such behaviour. This offers more proof that the TPB may be employed in cyber ethics studies. It demonstrates how the TPB may be used specifically with students from township high schools, many of whom originate from underserved rural communities and frequent domestic problems. The study also contributes to the body of knowledge by conceptualising cyber ethics among high school students within the context of the uMhlathuze Municipality.

## **6.6. Recommendations**

The following are the study's recommendations in order to fill the identified gaps.

### **6.6.1. To determine the level of awareness of cyber ethical behaviour among students at the selected high schools in uMhlathuze Municipality**

To reduce the misuse of cyber ethics in high schools, the teachers and principals need to implement programmes that will teach students about cyber ethics, that will increase the awareness of cyber ethics and reduce the harmful effects of cyber violations. It is much easier to raise awareness concerning intellectual property and copyrights, because some learners take subjects that teach about these topics. The teaching of cyber ethics in high schools is highly recommended: this could help students to minimise unethical behaviour in cyberspace. The study's proven findings and the necessity for cyber ethics education for students are both evident. The study recommends that Grade 11 students upward

should be trained on how to use information ethically as they are pre-matric and about to leave secondary schools to attend higher education institutions.

### **6.6.2. To identify the forms of cyber ethics behaviour revealed by the selected high school students.**

Cyberbullying, using another person's password and disseminating fake news are currently dominant in the studied schools. The study recommends that teaching of cyberbullying and other forms of cyber ethics in schools should be compulsory. Furthermore, the use of cyber technology should be taught in high schools since the students use cyber technologies to connect with their friends and for educational purposes. The findings of this study have shown that many users frequently do not adhere to the list of permissible behaviours on the Internet. The harmful effects of these forms of cyber ethics should be highlighted in schools, especially as some students in high schools end up committing suicide because of the things that have been said about them in cyberspace.

### **6.6.3. To demonstrate the application of the Theory of Planned Behaviour on cyber ethical behaviour intentions of high school students in Dlangezwa -High, Ongoye High and Empangeni High School**

This finding demonstrates that students were more involved in the tasks that utilising their cyber technology made simpler. This is done because of the fact that they lack the skills of using cyber technologies and some do not even know the harmful effects of misusing cyber ethics. The subjective norms happen to be the most dominant behaviour that pushes the students to post on social media and even use the Internet. The social pressure from peers is the cause of students using the Internet. Therefore, the study recommends that as the schools host programmes that educate them about cyber ethics, family and friends should be allowed to attend those programmes, especially parents, as they are the ones that spend a significant amount of time with the students. Subjective norms are an idea or concept of societal pressures from others who matter to them (e.g., family, friends, co-workers, and others) to act (or not) in a specific way, as well as their incentive to conform to other people's ideas (Ham, Jeger and Ivkovic, 2015:743).

#### **6.6.4. To determine the challenges faced by high school students to act ethically when using the Internet and computers at three selected high schools.**

A lack of legislation and enforcement exists to meet these many difficulties, also the lack of an adequate organisation to deal with cyber ethics misuse behaviour. There is a significant shortage of knowledge on cyber behaviour, and there have been breaches of network integrity and confidentiality; these indicated that students are facing significant challenges. The 21<sup>st</sup> century has made students use the 21<sup>st</sup>-century cyber technology for almost everything in their lives, especially connecting with their friends and families. The teaching of cyber ethics in schools is a necessity and limiting students on the time they spend on social media or using the cyber technology working along with the parents is essential. Making cyber ethics discussions a core component of school values will probably encourage ethical growth among students as a whole.

#### **6.7. Future studies**

Future research is needed to fill the voids indicated in current research and related studies about high school students' awareness of cyber ethics.

The below-mentioned studies should be undertaken in the future:

- Conduct a similar study in the future with the same schools to see if there is any improvement or growth in students' understanding of cyber ethics, and to determine if teachers are teaching enough about ethics in high schools.
- A comparative study between Grades 11 and 12 of these selected schools to check the level of awareness of learners regarding cyber ethics as they are about to leave the secondary schools to tertiary institutions and
- A study should be conducted on high schools under uMhlathuze Municipality.
- A study on the attitude and level of awareness of school instructors and principals regarding cyber ethical behaviour should be undertaken.



## **6.8. Summary**

The four research questions have various degrees of fulfilment in the answers. This study's objective is to encourage cyber ethics in the high school context, and it is meant to do so by offering several intervention options to the management of the participating schools. It is also hoped that numerous further studies on information ethics and cyber ethics will soon emerge to spur on more research. Therefore, it is recommended that further research should extend the Theory of Planned Behaviour to include situational aspects and empirically evaluate the concept. Further research should also be conducted on teachers and principals to examine their knowledge and awareness on cyber ethics especially in high schools.

## References

- Abaido, G., M. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, 25(1), 407-420.
- Acılar, A. and Aydemir, M. (2010). Students' attitudes towards software piracy the gender factor: a case of a public University in an emerging country. pp.2-8, Retrieved Online 16 June 2022. Available at SSRN: <https://ssrn.com/abstract=1703555>
- Aderibigbe, N., A. (2019). Cyberethical behaviour of undergraduate students of University of Zululand, South Africa, and the federal University of Agriculture, Abeokuta, Nigeria. Retrieved Online 13 May 2021 Available at <https://www.researchgate.net/publication/336073197/Ethical/Cyber/Behaviour/among/Undergraduate/students/in/Selected/African/Universities>
- Aderibigbe, A. (2021). Synopsis on cyber ethics behaviour: A literature review. *Inkanyiso, Journal of Humanities and Social Sciences*, 13(2).
- Aderibigbe, N., A, Ocholla, D., N (2020). Insight into ethical cyber behaviour of undergraduate students at selected African Universities. *SA Journal of Information Management*, 22(1).
- Aderibigbe, N., A, Ocholla, D., N. and Britz, J. (2021). Differences in ethical behavioural intention of Nigerian and South African students: A multi group analysis based on the Theory of Planned Behaviour. Accessed on 26/04/ 2022 Available at: <https://www.researchgate.net/publication/355701675>
- Aderibigbe, N., A. and Owolabi, K., A. (2020). Cyber ethical behaviour of university students: an overview of university of Zululand, South Africa and Federal university of Agriculture, Abeokuta, Ogun State, Nigeria. *Journal of applied information science technology*, 13(1), 87-106.
- Aduwa-Ogiegbaen, S., E. and Iyamu, E., O., S. (2005). Using information and communication technology in secondary schools in Nigeria: Problems and prospects. *Educational Technology and Society*, 8, 104-112.
- Ajzen, I. (2005). *Attitudes, Personality and Behaviour*. McGraw Hill: Open University Press.

Ajzen, I. (2011). The Theory of Planned Behaviour: *Reactions and Reflections*. *Psychology and Health*, 26(9), 1113-1127.

Ajzen, I. (1991). Theory of Planned Behaviour. *Organizational behaviour and human decision processes*, 50(2). 179-211, Retrieved Online 27 September 2022. available at <https://www.researchgate.net/publication/272790646>

Ajzen, I. (1993). Attitudes Theory and the Attitude Behaviour Relation. In D. Krebs, and P. Schidt (Eds.), *New Directions in Attitude measurement* (pp.41-57). Walter de Gruyter.

Ajzen, I. (1985). From intentions to Actions: A Theory of Planned Behaviour. In *Action control* (pp. 11-39). Berlin, Heidelberg: Springer.

Ajzen, I., and Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behaviour*. Englewood-Cliffs: Prentice-Hall.

Ajzen, I., Joyce, N., Sheikh, S. and Cote, N., G. (2011). Knowledge and the prediction of behaviour: The role of information accuracy in the Theory of Planned Behaviour. *Basic and Applied Social Psychology*, 33(2), 101-117.

Akbulut, Y., Şendağ, S., Birinci, G., Kılıçer, K., Şahin, M. C. and Odabaşı, H. F. (2008). Exploring the Types and Reasons of Internet-Triggered Academic Dishonesty among Turkish Students: Development of Internet-Triggered Academic Dishonesty Scale (ITADS). *Computers and Education*, 51(1), 463-473.

Aliyu., A. Bello., M., U. Kasim., R. and Martin., D. (2014). Positivist and non-positivist paradigm in social science research: Conflicting paradigms or perfect partners. *Journal of management and sustainability*, 4(3):79-95.

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D. and Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, Jakarta, 13-14 December. Retrieved 26 March 2022.

Al-Rafee, S. and Cronan, T.P. (2006). Digital piracy: Factors that influence attitude toward behaviour. *Journal of Business Ethics*, 63(3):237-259.

Armitage, C. and Conner, M. (2001). Efficacy of the theory of planned behaviour: a meta-analytic review. *British Journal of Social Psychology*, 40, 99-471.

Attuquayefio, S. and Addo, H. (2014). Using the UTAUT model to analyze students' ICT adoption. *International Journal of Education and Development using ICT*, 10(3), Open Campus, The University of the West Indies, West Indies. Retrieved 23 November, 2022 from <https://www.learntechlib.org/p/148478>

Bamberg, S. (2000). The promotion of new behaviour by forming an implementation intention result of a field experience in the domain of travel mode choice. *Journal of Applied Social Psychology*, 30.

Bansel, P., Davies, B., Laws, C. and Linnell, S. (2009). Bullies, bullying and power in the contexts of schooling. *British Journal of Sociology of Education* 30: 59–69.

Barakabitze, A., Lazaro, A. W., Alnea, N., Mkwiza, M. H., Maziku, H., Matofall, A. X., Iddl, A., Sanga, C. (2019). Transforming African education system in science, technology, engineering, and mathematics (STEM) using ICTs: Challenges and opportunities. *Education Research International*, vol. Retrieved Online on 31 October 2022. Available online at: <https://doi.org/10.1155/2019/6946809>

Bawa, D. S. and Marwah, A. (2011). Cyber ethics—A new evolving arena. *International Journal of Computer Science and Information Technology*, 1(6), 369-381.

Bear, L. (2014). 3 For Labour: A Jeet's Accident and the Ethics of Technological Fixes in Time. *Journal of the Royal Anthropological Institute*, 20, 71-88.

Beck, L. and Ajzen, I., (1991). Predicting dishonest actions using the theory of planned behaviour. *Journal of research in personality*, 25(3):285-301.

Bisquolm, S. (2010). A Theory of Planned Behaviour: In consideration of use in the field of low salary jobs recruitment. Accessed on 20 October 2022.

Bouhnik, D. and Deshen, M. (2014). WhatsApp Goes to School: Mobile Instant Messaging between Teachers and Students. *Journal of Information Technology Education: Research*, 13(1), 217-231.

- Bryman, A. (2012). *Social Research Methods*, 4th ed. Oxford: Oxford University Press.
- Burnard, P., Gill, P., Stewart, K., Treasure, E. and Chadwick, B. (2008). Analysing and presenting qualitative data, *British Dental Journal*, 204(8), 429-432.
- Bynum, T., W. (2008). Norbert Wiener and the arise of Information ethics. *Information technology and moral philosophy*. Cambridge University Press.
- Calvani, A., Fini, A., Ranieri, M. and Picci, P. (2012). Are young generations in secondary school digitally competent? A study on Italian teenagers. *Computers and Education*, 58(2):797-807
- Cassim, F. (2010). Addressing challenges posed by cybercrime: a South African Perspective. *Journal of International Commercial and Technology*, 5(3), 118-123.
- Cesareo, L. and Pastore, A. (2014). Consumers' Attitude and Behaviour Towards Online Music Piracy and Subscription-based Services. *Journal of Consumer Marketing*, 31(6/7), 515- 525.
- Chai, C., S, Wang, X. and Xu, C. (2020). An extended theory of Planned Behaviour for the Modelling of Chinese secondary school students' intention to learn Artificial Intelligence. *MDPI Journal Mathematics*, 8(11).
- Chan, H., C. O. and Wong, D. S. (2015). The Overlap between School Bullying Perpetration and Victimization: Assessing the Psychological, Familial, and School Factors of Chinese Adolescents in Hong Kong. *Journal of Child and Family Studies*, 24(11), 3224-3234.
- Chandarman, R., and Van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, 2017(20), 133-155.
- Chatterjee, S., Sarker, S., and Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, 31(4), 49-87. Retrieved Online: 06 June 2022. <https://doi.org/10.1080/07421222.2014.1001257>
- Chatterjee, S., Valacich, J. S. and Sarker, S. (2012). Unethical Use of Information Technology: A Two-country Study. In 2012 45th Hawaii *International Conference on System Sciences* (pp. 3071-3080). IEEE.

Chiang, L., and Lee, B. (2011). Ethical attitude and behaviours regarding computer use. *Ethics and Behavior*, 21(6):481-497.

Cilliers, L. (2017). Evaluation of Information Ethical Issues among Undergraduate Students: An Exploratory Study. *South African Journal of Information Management*, 19(1), 1-6. 19 October 2021 Available at: <https://doi.org/10.4102/sajim.v19i1.767>

Cohen, L., Manion, L. and Morrison, K. (2011). Surveys, Longitudinal, Cross-sectional and Trend Studies. *Research Methods in Education*, 7th edition. Abingdon: Routledge, 261-4.

Conner, M. and Sparks, P. (2005). Theory of Planned Behaviour and Health Behaviour. *Predicting Health Behaviour*, 2(1), 121-162.

Cooper, D. R., and Schindler, P. S. (2008). International Edition: Business Research Methods. New Delhi: McGraw-Hill.

Council of the European Union. (2015). Evaluation Report on the Seventh Round of Mutual Evaluations —The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime —Report on Slovakia, Brussels, 22 September 2015, 9761/1/15 REV 1 DCL 1

Creswell, J., W. (2012). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (4<sup>th</sup> ed.). Boston, MA: Pearson.

Creswell, J. W. (2014). A Concise Introduction to Mixed Methods Research. Sage Publications.

Creswell, J. W., and Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approach. Sage publications.

Cronan, T. P. and Al-Rafee, S. (2008). Factors That Influence the Intention to Pirate Software and Media. *Journal of Business Ethics*, 78(4), 527-545.

Cronan, T. and Douglas, D. (2006). Information technology ethical behaviour: towards a comprehensive ethical behaviour model. *Journal of Organizational and End User computing*, 18(1).

Dadzie, P.S. (2011). Rethinking information ethics education in Ghana: Is it adequate? *The International Information and Library Review*, 43(2):63-69.

- Dahlstrom, Eden, and Jacqueline Bichsel. (2014). ECAR Study of Undergraduate Students and Information Technology, 2014. Research Report. Louisville, CO: ECAR, October 2022. Available from <http://www.educause.edu/ecar>.
- Daraha, K. (2013). The effect of Internet use on high school students: a case study of Pattani province of Thailand. *Procedia-Social and Behavioural Sciences*, 91: 241-256
- Davies, B. (2011). Bullies as guardians of the moral order or an ethics of truths? *Children and Society* 25: 278–286.
- Davinson, N. and Sillence, E. (2010). It Won't Happen to Me: Promoting Secure Behaviour among Internet Users. *Computers in Human Behaviour*, 26(6), 1739-1747.
- DiScala, J. and Weeks, A., C. (2013). Access Denied: School Librarians' Responses to School District Policies on the Use of social media Tools. *School Library Research*, 16.
- Dixon, K. (2019). Social media's role in cyberbullying. Accessed on 15 December 2022. Available online at: <https://c-hit.org/2019/08/12/social-media-role-in-cyberbullying/>
- De Melo, C., and De Sousa, T. (2017). “Reflections on Cyberethics Education for Millennial Software Engineers.” In 2017 IEEE/ACM 1st International Workshop on Software Engineering Curricula for Millennials (SECM), 40–6. Buenos Aires: IEEE.
- Dudovskiy, J. (2018). The Ultimate Guide to Writing a Dissertation in Business Studies: a step-by-step approach. Germany: Usage.
- Duncan, N. (2013). ‘If you tolerate this, then your children will be next’. Compulsion, compression, control, and competition in secondary schooling. *International Journal on School Disaffection* 10: 29–45.
- Durrheim, K., and Painter, D. (2006). Collecting Quantitative Data: Sampling and Measuring. Applied Methods for Social Sciences. Cape Town: UCT Press.
- Dyck, B. and Wong, K. (2010). Corporate Spiritual Disciplines and the Quest for Organizational Virtue. *Journal of Management, Spirituality and Religion*, 7(1), 7-29.
- Directorate for Qualification and Standards in Education (DQSE). (2015). The Learning Outcomes Framework. Malta: Ministry for Education and Employment.

- Ebenezer, A. (2014). Migration of cybercrimes through cyber security and resilience in Nigeria. *International Journal of Topical issues*,1-12.
- Economic Commission for Africa. (2014). Annual report. United Nations: Digital Library.
- Edwards, A. (1957). Techniques of attitude scale construction. Appleton-century-crafts.
- Eisenstein, E., L. (1979). The printing press as an agent of change: communications and cultural transformations in early modern Europe, Cambridge University Press, 2(8).
- Eldakak, S. (2010). Does Applying Ethics in Education Have an Effective Impact in the Classroom? Online Submission.
- Eshetu, Y. (2017). Understanding cultural relativism: A critical: A critical appraisal of the theory. *International journal of multicultural and multireligious understating*, 4(6):24-30.
- Falconi, T. M. (2014). Global stakeholder relationships governance: An infrastructure. In Global stakeholder relationships Governance: An infrastructure (1-55). London: Palgrave Pivot.
- Ferrel, C., M. and Daniel, L., G. (1995). A frame of reference for understanding behaviors related to the academic misconduct of undergraduate teacher education students, *Research in Higher Education*, 36(3), 345–375.
- Festl, R. and Quandt, T. (2013). Social Relations and Cyberbullying: The Influence of Individual and Structural Attributes on Victimization and Perpetration via the Internet. *Human Communication Research*, 39(1), 101-126.
- Finn, M., Elliot-White, M., and Walton, M., (2000). Tourism and leisure research methods: Data collection, analysis and interpretation. London: Pearson Longman.
- Fishbein, M. and Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research
- Fishbein, M. and Ajzen, I. (2005). Theory-Based Behavior Change Interventions: Comments on Hobbis and Sutton. *Journal of Health Psychology*, 10(1), 27-31.
- Flick, U. (2015). Introducing research methodology: a beginner's guide to doing a research project. London: Sage



- Floridi, L. (2010). The Cambridge handbook of information and computer ethics. New York: Cambridge University Press.
- Frize, M. (2012). Electronic Medical Records (EMRs): Patient Safety and Ethical Considerations. *Ethics in Biology, Engineering and Medicine: An International Journal*, 3(1-3).
- Gagne, P. and Hancock, G. R. (2006). Measurement Model Quality, Sample Size, and Solution Propriety in Confirmatory Factor Models. *Multivariate Behavioural Research*, 41(1), 65-83.
- Galvez, S., M. and Guzman, I., R. (2009). Identifying Factors That Influence Corporate Information Security Behavior. AMCIS 2009 Proceedings, 765.
- Gentles, S. J., Charles, C., Ploeg, J., and McKibbin, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, 20(11), 1772-1789.
- Giaever, T. H., Mifsud, L., and Gjølstad, E. (2016). Teachers` Understanding and Practice of Understanding Cyber Ethics in the Classroom ICERI2016 Proceedings. 9th International Conference of Education, Research and Innovation, Retrieved Online: 25 May 2022. Available Online <https://library.iated.org/view/GIAEVER2016TEA>
- Gikenye, W. (2012). The Diffusion of Mobile Phones for Business and Information Management in Kenya. *Journal of Gender, Information and Development in Africa (JGIDA)*, 1(1), 43- 56.
- Ghada M., A. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates, *International Journal of Adolescence and Youth*. 25:1. 407-420. available online: <https://doi.org/10.1080/02673843.2019.1669059>
- Godin, G., Conner, M. and Sheeran, P. (2005). Bridging the Intention–Behaviour Gap: The Role of Moral Norm. *British Journal of Social Psychology*, 44(4), 497-512.
- Goles, T., Jayatilaka, B., George, B., Parsons, L., Chambers, V., Taylor, D. and Brune, R. (2008). Soft lifting: Exploring Determinants of Attitude. *Journal of Business Ethics*, 77(4), 481-499.
- Goundar, S. (2012). Chapter3: Research methodology and research method. (Ed.), Cloud computing. Research Gate Publications.
- Gowry, A. (2014). Research gap and research ethicsp. Kerala University of fisheries and oceans studies: SlideShare Company.

Gray, D., E. (Ed.). (2014). Doing research in the real world. University of Greenwich: Sage.

Gunarto, H. (2003). Ethical issues in cyberspace and IT society. Asia: Pacific University

Ham, M., Jeger, M. and Ivkovic, A., F. (2015). The role of subjective norms in forming the intention to purchase green food. Retrieved Online on 16 October 2022 Available online: <https://doi.org/10.1080/1331677X.2015.1083875>

Hanks, P. (Ed.). (1979). Collins Dictionary of the English Language. Glasgow: William Collins.

Hannes, K. (2019). Critical appraisal of qualitative research. New York: Cambridge Press.

Haughton, N. A., Yeh, K. C., Nworie, J. and Romero, L., (2013). Digital disturbances, disorders, and pathologies: A discussion of some unintended consequences of technology in higher education. *Educational Technology*: 3-16.

Harding, T. S., Mayhew, M. J., Finelli, C. J. and Carpenter, D. D. (2007). The Theory of Planned Behaviour as a Model of Academic Dishonesty in Engineering and Humanities Undergraduates. *Ethics and Behaviour*, 17(3), 255-279.

Harris, M. and Furnell, S. (2012). Routes to Security Compliance: Be Good or Be Shamed? *Computer Fraud and Security*, 2012(12), 12-20.

Head, K., and S. Noar. 2014. "Facilitating Progress in Health Behaviour Theory Development and Modification: The Reasoned Action Approach as a Case Study." *Health Psychology Review* 8 (1): 34–52.

Heller, V. (2012). Technology readiness level approach for the development of WECs. London: Imperial College.

Honebein, P., C. (1996). Seven goals for the design of constructivist learning environments. In Wilson, Brent. G. (Ed). (1996) Constructivist learning environments: Case studies in instructional design. Educational Technology Publications. New Jersey: Englewood Cliffs.

Horton, P. (2011). School bullying and social and moral orders. *Children and Society* 25: 268–277.

Ibrahim, S. (2016). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44-57.

In, J. (2017). Introduction of a pilot study. *Korean Journal of Anesthesiology*. 70(6), 601-605.

International research. (2019). What is quantitative research? [Online]. Available at: <https://www.sisinternational.com/what-is-quantitative-research/> [Accessed on 20 February 2021].

Irshad, S. and Soomro, T., R. (2018). Identity theft and social media. *International Journal of Computer Science and Network Security*, 18(1), 43-55.

Iyadat, W., Iyadat, Y., Ashour, R. and Khasawneh, S. (2012). University Students and Ethics of Computer Technology Usage: Human Resource Development. *E-Learning and Digital Media*, 9(1), 43-49

Jahankhani, H., Al-Nemrat, A, and Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. Retrieved online on 29 October 2022. Available at: <https://www.researchgate.net/publication/280488873>

Jamal, A., A, Ramlan, K., W, Karim, M., A, Mohidin, R. and Osman, Z. (2015). The effects of social influence and financial literacy on savings behaviour: a study on students of higher learning institution in Kota Kinabalu, Sabah. *International Journal of Business and Social Sciences*, 6 (11,1), 110-119.

Johnson, D., G. and Moor, G. (1985). Computer ethics. Englewood: Cliffs (NJ).

Kaplan, D. (2005). Broadcast flags and the war against digital television piracy: a solution or dilemma for the digital era. *Federal Communications Law Journal*, 57(2), 325.

Kavuk, M., Keser, H. and Teker, N. (2011). Reviewing Unethical Behaviours of Primary Education Students' Internet Usage. *Procedia-Social and Behavioural Sciences*, 28, 1043-1052.

Khalil, O, E. and Seleim, A. A. (2012). Attitudes towards Information Ethics: A View from Egypt.

Kleinrock, L. (2009). UCLA Computer Science Department. Los Angeles: Boelter Hall.

Kizza, J., M. (2013). Ethical and social issues in the information age. London: Springer.

Kofoed J, Sondergaard, D., M. (2009). Mobning. Sociale Processer på Afveje. (eds.). Hans Reitzels Forlag: København, Denmark

Kowalski, R., Giumetti, G., Schroeder, A. and Lattanner, M. (2014). Bullying in the Digital Age: a critical review and meta-analysis of Cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073-1137.

Kothari, C.R. (2004). *Research methodology: methods and techniques*. New Delhi: New age international (p) limited publishers. [ebook]. Accessed on 22 March 2021. Available at: <http://www2.hcmuaf.edu.vn/data/quoctuan/Research%20Methodology%20%20Methods%20and%20Techniques%202004.pdf> [].

Kortjan, N. and Von Solms, R. (2013). Cyber Security Education in Developing Countries: A South African Perspective. In: Jonas, K., Rai, I.A., Tchunte, M. (eds) *e-Infrastructure and e-Services for Developing Countries*. AFRICOMM 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 119. Springer, Berlin, Heidelberg. Accessed on 27 August 2022. [https://doi.org/10.1007/978-3-642-41178-6\\_30](https://doi.org/10.1007/978-3-642-41178-6_30)

Kreie, J. and Cronan, T., P. (2000). Making ethical decisions. *Communications of the ACM*, 43(12).

Krejcie, R., V. and Morgan, D., W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607-610.

Kruger, R. (2003). Discussing cyber ethics with students is critical. *The Social Studies*, Washington, 94(4), 188

Kuan, L. H., Idrus, R. and Mutton, N. A. R. (2015). Cyber ethics Awareness Using Defining Issues Test: A Preliminary Findings.

Kumar, R. (2019). *Research methodology: A step-by-step guide for beginners*. Sage Publications Limited.

Lau, W.W. and Yuen, A.H., 2014. Internet ethics of adolescents: Understanding demographic differences. *Computers and Education*, 72,378-385.

Ledwaba, L., S. (2018). *Provision of internet access to public libraries in South Africa*. Pretoria: University of South Africa.

- Leonard, L., N. and Cronan, T. (2005). Attitude toward Ethical Behaviour in Computer Use: A Shifting Model. *Industrial Management and Data Systems*, 105(9), 1150- 1171.
- Leonard, M., Graham, S. and Bonacum, D. (2004). The Human Factor: The critical importance of effective teamwork and communication in proving safe care. *Quality and Safety in Health Care*, 13, 85-90.
- Leslie, D., A. (2014). Cyberlaundering: concept and practice. In: Legal Principles for Combatting Cyberlaundering. Law, Governance and Technology series, 19. Springer International Publishing.
- Liao, C., Lin, H. N. and Liu, Y. P. (2010). Predicting the Use of Pirated Software: A Contingency Model Integrating Perceived Risk with the Theory of Planned Behaviour. *Journal of Business Ethics*, 91(2), 237-252.
- Liao, Q., Gurung, A., Luo, X. and Li, L. (2009). Workplace management and employee misuse: does punishment matter. *Journal of Computer Information Systems*, 50(2), 49-59.
- Lichtman, D. (2004). Holding internet service providers accountable. *Regulation, Washington*, 27(4), 54.
- Lin, C., S. and Chen, C. (2011). Application of Theory of Planned Behaviour on the study of workplace dishonesty. *International Conference on Economics, Business and Management*, 2, 66-69.
- Luppigini, R. (2009). Technoethical inquiry: from technological systems to society. *Global media Journal*.
- Maat, S., M. (2009). Cybercrime chapter 3. Unisa institutional repository: Accessed on 14 September 2022. Available from: <http://www.uir.unisa.ac.za>.
- Maphoto, A., R. (2016). Information needs information seeking behaviour of grade 10 and 11 learners at Gerson Njtie secondary school at gaMagooa village, Limpopo province. Pietermaritzburg: University of KwaZulu-Natal
- Maree, K, (Ed.). (2010). First steps in research. Pretoria: Van Schaik Publishers.
- Maree, K. (Ed.). (2016). First steps in research. Braamfontein: Van Schaik Publishers

- Mbanaso, U. and Dandaura, E. (2015). The cyberspace: redefining a new world. *Journal of Computer Engineering*, 17(3), 17-24.
- McCabe, D. L., and Trevino, L. K. (1997). Individual and Contextual Influences on Academic Dishonesty: A Multicampus Investigation. *Research in Higher Education*, 38(3), 379-396.
- McEachan, R. R. C., Conner, M., Taylor, N. J. and Lawton, R. J. (2011). Prospective Prediction of Health-Related Behaviours with the Theory of Planned Behaviour: A Meta-Analysis. *Health Psychology Review*, 5(2), 97-144.
- McMillan, J.H. and Schumacher, S. (1993). Research in Education: A conceptual introduction. New York: Collins Publishers.
- Meng, X. (2013). Scalable simple random sampling and stratified sampling. Proceedings of the 30th International Conference on Machine Learning, PMLR 28(3):531-539.
- Mertens, D.M. (2012). Ethics in qualitative research in education and the social sciences. In Lapan, S.D., Quartaroli, M.T. and Riemer, F.J, (eds.) Qualitative research: an introduction to methods and designs. London: Sage, pp. 19-39.
- Milton, J., Giaever, T., H, Mifsud, L, and Gasso, H., H. (2021). Awareness and knowledge of cyber ethics: A study of pre-service teachers in Malta, Norway and Spain. *Nordic Journal of comparative international education*, 5(4):18-37
- Mintzberg, H. (2017). Developing Theory about the Development of Theory. In Handbook of Middle Management Strategy Process Research. Edward Elgar Publishing. DOI:
- Moeini, S. (2014). 6 (Very Useful!) Approaches to identify research gaps and generate research questions.
- Molnar, K. K., Kletke, M. G. and Chongwatpol, J. (2008). Ethics vs. IT Ethics: Do Undergraduate Students Perceive a Difference? *Journal of Business Ethics*, 83(4), 657-671.
- Moor, J. H. (2001). The Future of Computer Ethics: You Ain't Seen Nothin' Yet! *Ethics and Information Technology*, 3(2): 89-91.
- Moor, J. H. (1985). What Is Computer Ethics? *Meta philosophy*, 16(4), 266-275.

- Moross, K. (2017). Cyberbullying: Youth's Perceptions in a Johannesburg School Context (Doctoral dissertation).
- Moskowitz, S. (2017). Cybercrime and Business: Strategies for Global Corporate Security. Butterworth-Heinemann.
- Mthembu, M. S. (2019). Job requirements and challenges of LIS graduates in public libraries in KwaZulu-Natal, South Africa. KwaDlangezwa: University of Zululand.
- National Crime Prevention Council. (2019). Bullying. Retrieve Online 22 May 2022. Available Online at: <https://wwwncpc.org/resources/bullying/>
- National Cyber Security Alliance. (2009) National Cyberethics, Cybersafety, Cybersecurity Baseline Study. Retrieved Online: 23 May 2022. Available Online: <http://staysafeonline.mediaroom.com/index.php?s=67&item=44>
- Neighbors, C. and Fossos, N. (2013). Peer influences on Addiction. *Comprehensive Addictive Behaviours and Disorders*, 1, 323-331.
- Neuman, W., L., (2011). Social research methods: Qualitative and quantitative approaches. 6th edition. Boston: Pearson Education.
- Ngoqo, B. and Flowerday, S. (2014). Linking student information security awareness and behavioural intent. UK: ResearchGate.
- Ngulube, P. (2015). Trends in Research Methodological Procedures Used in Knowledge Management Studies. *Afr. J. Lib. Arch. And Inf. Sc*, 25(2):125-143.
- Notar, C., E, Padgett, S. and Roden, J. (2013). Cyberbullying: resources for intervention and prevention. *Universal Journal of Education Research*, 1(3), 133-137.
- Ocholla, D. (2009). Information Ethics Education in Africa. Where Do We Stand? *The International Information and Library Review*, 41(2), 79-88.
- Ocholla, D. N. and Le Roux, J. (2011). Conceptions and misconceptions of theoretical frameworks in Library and Information Science research: a case study of selected theses and dissertations from eastern and southern African universities. *Mousaion*, 29(2), pp.61-74.

- Ogden, J. (2003). Some problems with social cognition models: A pragmatic and conceptual analysis. *Health Psychology*, 22(4), 424-428. 06 May 2021. Available at: <https://doi.org/10.1037/0278-6133.22.4.424>
- Osanloo, A. and Grant, C. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for your house. *Administrative Issues Journal: Connecting Education, Practice, and Research*, 4(2), 12-26.
- Oskamp, S. (1977). Attitudes and opinions: Clinical and social psychology series. Harvard University: Prentice-Hall.
- Oyewole, O. (2017). Awareness and perception of computer ethics by undergraduates of a Nigerian University. *Journal of Information Science Theory and Practice*, 5 (4), 68-80.
- Ozer, N., Ugurlu, C., T. and Beycioglu, K. (2011). Computer teachers' attitudes toward ethical use of computers in Elementary schools. *International Journal of Cyber Ethics in Education*, 1(2), 15-24.
- PA Media Group. (2020). The use of electronic devices by young people. News agency company.
- Pallant, J. (2013). SPSS Survival Manual. McGraw-Hill Education (UK).
- Park, C. (2003). In Other (People's) Words: Plagiarism by university students--literature and lessons, *Assessment and Evaluation in Higher Education*, 28:5, 471-488. Retrieved Online on 28 November 2022. Available at: <https://doi.org/10.1080/02602930301677>
- Pascoe, G. (2014). Sampling: Research matters. Cape Town: Juta.
- Peace, A. G., Galletta, D. F. and Thong, J. Y., (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, 20(1):153-177
- Peng, T. Q., Zhu, J. J., Tong, J. J. and Jiang, S. J. (2012). Predicting Internet Non-Users' Adoption Intention and Adoption Behavior: A Panel Study of Theory of Planned Behavior. *Information, Communication and Society*, 15(8), 1236-1257.
- Perez, A. and Choi, Y. (2007). Online piracy, Innovation, and Legitimate business models. 27(4), 168-178. Accessed Online on 28 November 2022. Available at: <https://doi.org/10.1016/j.technovation.2006.09.004>



- Petersen, T., S and Ryberg, J. (2010). Applied ethics. Accessed online on 26 April 2022. Available at: [\(PDF\) Applied Ethics \(researchgate.net\)](#)
- Phillips, D., C. and Burbules, N., C. (2000). Postpositivism and educational research. Rowman and Littlefield.
- Pickard, A.J. (2007). Research methods in information. London: Facet Publishing
- Plaisance, P., L. (2013). Media ethics. International Encyclopaedia of Ethics, 1-11.
- Polkowski, Z. (2015). Ethical issues in the use and implementation of ICT. *Journal of management and research*, 21(2): 2-5.
- Power, C. (2014). The power of education: educating for all, development, Globalisation and UNESCO. Australia: Springer.
- Prathapan, K. (2014). Research methodology for scientific research. I.K. International publishing house: New Delhi.
- Puspita, R., A. and Rohedi, D. (2018). The impact of internet use for students. Materials Science and Engineering.
- Raffetto, W., G. (1985). The cheat. *Community and Junior College Journal*, 56 (2), 26–27.
- Rasmitadila, R., Aliyya, R., R., Rachmadtullah, R., Samsudin, A., Syaodin, E., Nurtanto, M. and Tambunan, A., R., S. (2020). The perceptions of primary school teachers of online learning during the Covid-19 pandemic period: A case study in Indonesia. *Journal of Ethnic and Cultural Studies*, 7(2), 90-109.
- Reddy, G., N. and Reddy, G., J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. *International Journal of Engineering and Technology*, 4(1).
- Ridley, D. (2012). The literature review: A step by step guide for students. UK: Sage.
- Roopa, S. and Rani, M., S. (2012). Questionnaire designing for a survey. *The Journal of Indian Orthodontic Society*, 46(4), 273-277.
- Rujoiu, O. and Rujoiu, V. (2014). Academic Dishonesty and Workplace Dishonesty: An Overview. In Proc. Int. Manage. Conference, 8, 928-938.

- Russo, D., Stochl, J., Painter, M. and Shelley, G. (2015). Use of the Theory of Planned Behaviour to assess factors influencing the identification of students at clinical high risk for psychosis in 16+ education. *BMC Health Services Research* 15(1):411
- Sahin, Y. G. Balta, S. and Ercan, T. (2010). The use of internet resources by university students during their course project elicitation: A case study. *Journal of educational technology*, 9(2):234-244.
- Sarua, (2019). University of Zululand: History. Retrieved Online 22 May 2022. Available at: <https://www.sarua.org/?Q=content/university-zululand-history>
- Schultz, C., B. (2017). Cybercrime: an analysis of current legislation in South Africa. University of Pretoria: Pretoria.
- Schweitzer, D., Gibson, D., Bibighaus, D. and Boleng, J. (2009). Preparing Our Undergraduates to Enter a Cyber World. In *IFIP World Conference on Information Security Education* (pp. 123-130). Springer, Berlin, Heidelberg.
- Shapiro, S and Gross, S. J. (2013). Ethical educational leadership in turbulent times: resolving moral dilemmas. Retrieved on 05 September 2022. Available online at [Ethical Educational Leadership in Turbulent Times: \(Re\)Solving Moral Dilemmas | Request PDF \(researchgate.net\)](#)
- Soomro, T., R. (2018). Identity theft. Accessed online on 20 October 2022. Available at: <https://www.researchgate.net/publication/323185128>
- Sommer, L. (2011). The Theory of Planned Behaviour and the Impact of Past Behaviour. *International Business and Economics Research Journal*, 10(1), 91-110.
- Snyder, I., Jones, A. and Bianco, J. (2005). Using Information and Communication Technologies in Adult Literacy Education: New Practices, New Challenges. An Adult Literacy National Project Report. National Centre for Vocational Education Research Ltd. PO Box 8288, Stational Arcade, Adelaide, SA 5000, Australia
- Stahl, B., C., Eden, G. and Jirotko, M. (2013). Responsible research and innovation in information and communication technology: Identifying and engaging with the ethical implications of ICTs. *Responsible innovation*, 199-218.

- Statista. (2014). Distribution of Daily Media Consumption among 15–24-Year-Olds in the United Kingdom (UK) in 2014. Accessed online 17 September 2022. Retrieved at from: <https://www.statista.com/statistics/486125/daily-media-diet-of-young-people-uk/>
- Stone, T. H., Jawahar, I., M. and Kisamore, J., L. (2010). Predicting academic misconduct intentions and behaviour using the theory of planned behaviour and personality. *Basic and Applied Social Psychology*, 32(1):35-45.
- Struwig, F., W and Stead, G., B. (2001). Planning, designing, and reporting research. Cape town: Pearson Education.
- Stylianou, A. C., Winter, S., Niu, Y., Giacalone, R. A. and Campbell, M. (2013). Understanding the Behavioural Intention to Report Unethical Information Technology Practices: The Role of Machiavellianism, Gender and Computer Expertise. *Journal of Business Ethics*, 117(2), 333-343.
- Supavai, E. (2014). Measuring Online Moral Reasoning: The Development and Psychometric Properties of the Cyber Ethics Scale (Doctoral Dissertation, Boston University)
- Taylor, S. and Todd, P., A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2): 144-176.
- Tavani, H. T. (2013). Cyberethics. In: Runehov A.L.C., Oviedo L. (eds). *Encyclopaedia of Sciences and Religions*. Dordrecht: Springer.
- Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and Ransomware attacks. *International Journal of Business and Management*. Accessed Online 13 December 2022. Available Online at: <https://www.researchgate.net/publication/32486314>
- Truong, Y. (2009). An evaluation of the Planned Behaviour in Consumer Acceptance of Online Video and Television Services. *The Electronic Journal Information Systems Evaluation*, 12(2), 177-186.
- Udo-Akang, D. (2013). Ethical Orientation for New and Prospective Researchers. *American International Journal of Social Science*, 2(1), 54-64.

University of North Carolina. (2014). General Administration. Student Services: Responding to Issues and Challenges: The Fifth Compendium of Papers. University of North Carolina General Administration.

Vallor, S. (2010). Social networking technology and the virtues. *Ethics and Information technology*, 12(2), pp.157-170.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 425-478.

Von Schomberg, R. (2012). Prospects for Technology Assessment in a Framework of Responsible Research and Innovation. In *Technikfolgen abschätzen lehren* (pp. 39- 61). VS Verlag für Sozialwissenschaften.

Wagner, S. C. and Sanders, G. L. (2001). Considerations in Ethical Decision-Making and Software Piracy. *Journal of Business Ethics*, 29(1-2), 161-167.

Walczak, K., Finelli, C., Holsapple, M., Sutkus, J., Harding, T. and Carpenter, D. (2010). Institutional Obstacles to Integrating Ethics into the Curriculum and Strategies for Overcoming Them.

Wall, D., S. (2007). *Cybercrime: The transformation of crime in information age*. Polity Press.

Williman, N. (2011). *Research methods: The basics*. Routledge.

Yamano, T. and Jayne, T., S. (2004). Measuring the impact of working age adult morality on small scale farm household in Kenya. *Journal of World Development*, 32(1), pp1-190.

Yan, Z. (Ed.). (2012). *Encyclopaedia of Cyber Behaviour* (Vol. 1). IGI Global.

Yaokumah, W. (2020). Predicting and Explaining Cyber Ethics with Ethical Theories. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 10(2), 46-63. Retrieved Online 12 December 2022. Available at: <http://doi.org/10.4018/IJCWT.202004010>

Yoon, C. (2010). Ethical Decision-Making in the Internet Context: Development and Test of an Initial Model Based on Moral Philosophy. *Computers in Human Behaviour*, 27(6), 2401- 2409.

## APPENDICES

### Appendix 1: Ethical clearance letter



**UNIVERSITY OF ZULULAND RESEARCH  
ETHICS COMMITTEE**  
(Reg No: UZREC 171110-030)

**ETHICAL CLEARANCE CERTIFICATE**

<b>Certificate Number</b>	UZREC 171110-030 PGM 2021/121				
<b>Project Title</b>	CYBERETHICAL BEHAVIOUR OF HIGH SCHOOL STUDENTS IN THE SELECTED SCHOOLS IN UMHLATHUZE MUNICIPALITY				
<b>Principal Researcher/ Investigator</b>	N.N. Buthelezi				
<b>Supervisor and Co-supervisor</b>	Prof Ocholla		Ms LP Luthuli		
<b>Department</b>	Information Studies				
<b>Faculty</b>	Humanities and Social Sciences				
<b>Type of Risk</b>	Medium Risk - Data collection from people				
<b>Nature of Project</b>	Honours/4 <sup>th</sup> Year		Master's	x	Doctoral
					Departmental

The University of Zululand's Research Ethics Committee (UZREC) hereby gives ethical approval in respect of the undertakings contained in the above-mentioned project. The Researcher may therefore commence with data collection from the date of this Certificate, using the certificate number indicated above.

SPECIAL CONDITIONS. (i) This certificate is valid for 1 year from the date of issue.

(2) Principal researcher must provide an annual report to the UZREC in the prescribed format [due date- 22 July 2023]

(3) The UZREC must be informed immediately of any material change in the conditions or undertakings mentioned in the documents that were presented to the meeting.

(4) Under the Protection of Personal Information Act, 04 of 2013 ("POPIA"), researchers have a general legal duty to protect the information they process. They must ensure the security and protection of any personal information processed through the research and provide a compliant and consistent approach to data protection. The information collected via interviews must be for research purposes only. No personal

information such as opinions, views, and academic background may be linked to the respondents' identity or shared with anyone for marketing purposes or otherwise.

The



UZREC wishes the researcher well in conducting research,

**CHAIRPERSON  
UNIVERSITY OF ZULULAND RESEARCH  
ETHICS COMMITTEE (UZREC)  
REG NO: UZREC 171110-30**

**2022 -07- 2 2.**

**RESEARCH & INNOVATION OFFICE**

Prof. Nokuthula Kunene

Chairperson: University Research Ethics Committee Deputy Vice-Chancellor: Research & Innovation 22 July 2022

## RESEARCH INNOVATION OFFICE

Website:

Private Bag X1001

KwaDlangezwa. 3886

Tel: 035 902 6374/6324

Email: [MthembuNL@unizulu.ac.za](mailto:MthembuNL@unizulu.ac.za) / [MangeleS@unizulu.ac.za](mailto:MangeleS@unizulu.ac.za)

## APPENDIX 2: DEPARTMENT OF EDUCATION APPROVAL LETTER



**KWAZULU-NATAL PROVINCE**

**EDUCATION  
REPUBLIC OF SOUTH AFRICA**

**OFFICE OF THE HEAD OF DEPARTMENT**

**ENQUIRIES: PHINDILE DUMA**

**REF.:2/4/8/4090**

MS NN BUTHELEZI

B2433 SAGILA ROAD

**KWAMASHU**

4360

DEAR MS BUTHELEZI

**PERMISSION TO CONDUCT RESEARCH IN THE KZN DOE INSTITUTIONS**

YOUR APPLICATION TO CONDUCT RESEARCH ENTITLED: **“CYBERETHICAL BEHAVIOUR OF HIGH SCHOOL STUDENTS IN THE SELECTED SCHOOLS IN UMHLATHUZE MUNICIPALITY”**, IN THE KWAZULU-NATAL DEPARTMENT OF EDUCATION INSTITUTIONS HAS BEEN APPROVED. THE CONDITIONS OF THE APPROVAL ARE AS FOLLOWS:

1. THE RESEARCHER WILL MAKE ALL THE ARRANGEMENTS CONCERNING THE RESEARCH AND INTERVIEWS.
2. THE RESEARCHER MUST ENSURE THAT EDUCATOR AND LEARNING PROGRAMMES ARE NOT INTERRUPTED.
3. INTERVIEWS ARE NOT CONDUCTED DURING THE TIME OF WRITING EXAMINATIONS IN SCHOOLS.
4. LEARNERS, EDUCATORS, SCHOOLS AND INSTITUTIONS ARE NOT IDENTIFIABLE IN ANY WAY FROM THE RESULTS OF THE RESEARCH.
5. A COPY OF THIS LETTER IS SUBMITTED TO DISTRICT MANAGERS, PRINCIPALS AND HEADS OF INSTITUTIONS WHERE THE INTENDED RESEARCH AND INTERVIEWS ARE TO BE CONDUCTED.
6. THE PERIOD OF INVESTIGATION IS LIMITED TO THE PERIOD FROM 06 JUNE 2022 TO 30 MAY 2025.
7. YOUR RESEARCH AND INTERVIEWS WILL BE LIMITED TO THE SCHOOLS YOU HAVE PROPOSED AND APPROVED BY THE HEAD OF DEPARTMENT. PLEASE NOTE THAT PRINCIPALS, EDUCATORS, DEPARTMENTAL OFFICIALS AND LEARNERS ARE UNDER NO OBLIGATION TO PARTICIPATE OR ASSIST YOU IN YOUR INVESTIGATION.
8. SHOULD YOU WISH TO EXTEND THE PERIOD OF YOUR SURVEY AT THE SCHOOL(S), PLEASE CONTACT MISS PHINDILE DUMA AT THE CONTACT NUMBERS ABOVE.

9. UPON COMPLETION OF THE RESEARCH, A BRIEF SUMMARY OF THE FINDINGS, RECOMMENDATIONS OR A FULL REPORT/DISSERTATION/THESIS MUST BE SUBMITTED TO THE RESEARCH OFFICE OF THE DEPARTMENT. PLEASE ADDRESS IT TO THE OFFICE OF THE HOD, PRIVATE BAG X9137, PIETERMARITZBURG, 3200.
10. PLEASE NOTE THAT YOUR RESEARCH AND INTERVIEWS WILL BE LIMITED TO SCHOOLS AND INSTITUTIONS IN KWAZULU-NATAL DEPARTMENT OF EDUCATION.

**KING CETSHWAYO DISTRICT**



**MR GN NGCOBO**

**HEAD OF DEPARTMENT: EDUCATION**

**DATE: 08 JUNE 2022**

**GROWING KWAZULU-NATAL TOGETHER**

### **APPENDIX 3: INFORMED CONSENT LETTER**

Department of Information Studies,  
University of Zululand,  
P/B X1001,  
KwaDlangezwa,  
3886

Dear participant

I am **Buthelezi Noxolo Nqobile** a master's student in the Department Information Studies at the University of Zululand, conducting a study on cyberethical behaviour of high school students in selected schools in uMhlathuze Municipality.



Therefore, you are kindly requested to contribute to this particular study. Your contribution in this study will empower the researcher to indicate your sight of these modules as a registered student in the LIS field.

Your participation in this study is voluntary, meaning that you are not enforced to reveal any of your information and confidentiality is certain. You are free to withdraw from this study at any moment of your choice. Your identity and your personal information in any document, including in the research report, will remain anonymous.

For any queries about the study, you are welcome to contact the researcher at the following contact details or email address. Your participation is highly appreciated!

Yours truly,

Buthelezi Noxolo Nqobile

Cell phone number : 0665904446

Email address : [nqobileshoti@gmail.com](mailto:nqobileshoti@gmail.com)

Please specify your agreement in contribution of this study by signing this form.

Participant's consent

Name.....

Signature.....

Date.....

For more information, please contact me or my supervisor on the following contact details:

**Co-Supervisor: Ms. L.P Luthuli**

Email: [NgidiL@unizulu.ac.za](mailto:NgidiL@unizulu.ac.za)

**2. Supervisor: Prof D.N Ocholla**

Email: [OchollaD@unizulu.aca.za](mailto:OchollaD@unizulu.aca.za)

## APPENDIX 4; PARENTAL CONSENT LETTER

Department of Information Studies,  
University of Zululand,  
P/B X1001,  
KwaDlangezwa,  
3886

Dear Parent

My name is Noxolo Buthelezi from the Department of Information Studies, University of Zululand. My contact details are as follows: 0665904446/nqobileshoti@gmail.com. Your child is being invited to consider participating in a study that is about cyber ethical behaviour of high school students in the selected schools in uMhlathuze Municipality.

The aim of this is to examine the unethical cyber behaviour of high school students in the three selected schools in uMhlathuze Municipality and gain knowledge of the factors that lead to such behaviour.

The study is expected to enrol 214 Grade 11 learners of KwaDlangezwa High, Ongoye HHigh as well as Empangeni High School. Simple random sampling will be used to ensure that learners have equal chances of being chosen for participation.

The duration of participation if you allow your child to enrol and remain in the study is expected to be about 10 minutes. Participants will receive no direct benefits from the study.

The participation of your child in this study is voluntary, meaning that they are not forced to reveal any of their information and confidentiality is guaranteed. Their identity and personal information in any document, including in the research report, will remain anonymous.

For any queries about the study, you are welcome to contact the researcher at the following contacts details or email address. Your participation is highly appreciated!

Yours truly,

Buthelezi Noxolo Nqobile

Please specify your agreement to contribute to this study by signing this form.

Parent's consent

Name.....

Signature.....

Date.....

For more information, please contact me or my supervisor on the following contact details:

**Researcher:** Ms. N.N Buthelezi

Email: [nqobileshoti@gmail.com](mailto:nqobileshoti@gmail.com)

Cellphone no: 067 279 4746

**Co-Supervisor:** Dr. L.P Luthuli

Email. [NgidiL@unizulu.ac.za](mailto:NgidiL@unizulu.ac.za)

Telephone: 035 902 6810

**Supervisor:** Prof D.N Ocholla

Email: [OchollaD@unizulu.ac.za](mailto:OchollaD@unizulu.ac.za)

[Telephone: 082 372 4638](tel:0823724638)

## APPENDIX 5: LETTER SEEKING AUTHORITY TO CONDUCT A STUDY

Faculty of Humanities and Social Sciences

University of Zululand

P/B X1001

KwaDlangezwa

3886

TO WHOM IT MAY CONCERN

**RE: Introducing Miss Buthelezi Noxolo Nqobile – Masters Student at University of Zululand**

This letter serves to confirm that **Miss Buthelezi N.N** is a registered master's student in the Information Studies Department at the University of Zululand. The title of her research is '**Cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality.**

The result of the study is expected to advance practice, inform policy and extend theory in this particular field of study. As part of the requirements for the award of a master's degree, she is required to undertake original research in a setting and location of her choice. The UNIZULU ethical compliance principles require her to provide proof which can be a letter or email that the appropriate authority where the research is to be undertaken has given approval.

Your support and understanding to grant Miss Buthelezi Noxolo Nqobile permission to carry out research in your organization is appreciated. For any further clarification, do not hesitate to contact myself or Miss Buthelezi

Thank you in for your consideration.

Yours sincerely,

**.Co-Supervisor:** Ms. L.P Luthuli

Email: NgidiL@unizulu.ac.za

**Supervisor:** Prof D.N. Ocholla

Email: [OchollaD@unizulu.ac.za](mailto:OchollaD@unizulu.ac.za)

Noxolo Nqobile Buthelezi (Researcher)

Email: [nqobileshoti@gmail.com](mailto:nqobileshoti@gmail.com)

Cell: 0665904446

## APPENDIX 6: DATA COLLECTION INSTRUMENTS

### RESEARCH INSTRUMENT: A QUESTIONNAIRE

Cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality.

#### QUESTIONNAIRE GUIDE FOR STUDENTS

Dear respondent,

I am **Buthelezi Noxolo Nqobile** from **University of Zululand** currently undertaking **Masters' degree in Library and Information sciences**. I am investigating the study topic titled: *“Cyber ethical behaviour of high school students in selected schools in uMhlathuze Municipality”*. As part of the requirements for the completion of the master's degree. I kindly request your participation in my research project by completing this questionnaire. Be assured that all information provided/shared will be used for research purposes only. Anonymity and confidentiality will be observed. I respectfully request that you take part in this study; your contribution will be significantly appreciated, and I look forward to sharing the results of the study with you.

For any enquiries, please do not hesitate to contact us:

1. **Co-Supervisor:** Ms. L.P Luthuli

Email: NgidiL@unizulu.ac.za

Cell: 061 435 3591

2. **Supervisor:** Prof D.N Ocholla

Email: [OchollaD@unizulu.ac.za](mailto:OchollaD@unizulu.ac.za)

3. **Researcher:** Noxolo Buthelezi

Email: nqobileshoti@gmail.com

Cell: 0665904446

Thank you. I guarantee that your identity will remain secret, and this study is merely conducted for academic purposes.

Kindly fill in using a black pen and in the provided boxes kindly use crosses (X) or ticks (✓) to identify your response.

## **1. SECTION A: Background**

(a) Gender

Male	
Female	

(b) Age range

14-16	
17-20	
21+	

(c) Race Group

African	
White	
Indian	
Coloured	
Other	

(d) Which grade are you doing?

Grade 11 A or B	
Grade 11 C or D	
Other	

If you chose other, please specify which grade

.....

(e) Name of the high school

KwaDlangezwa High	
Ongoye High	
Empangeni High	

(f) How many years you have been in that grade?

Less than a year	
1 year	
2 years or more	

(g) Cyber technology skills

Beginning	
Intermediate	
Advanced	

## **2. Awareness and types of cyber ethical behaviour**

(a) Are you aware of cyber ethical behaviour?

Yes	
No	

(b) Do you think your school teaches enough about cyber ethics?

Yes	
No	
Sometimes	

(c) Why do you think so?

.....

.....

.....

(d) The table below contains a list of cyber ethical behaviours. Please tick (✓) any of the cyber behaviours that you are familiar with.

NO	Cyber ethical behaviour	
1.	Cybersquatting	
2.	Cyberbullying	
3.	Cybercrime	
4.	Cyberstalking	
5.	Cyber vandalism	
6.	Cybersex (Online porn and pornography)	
7.	Cyber fraud	
8.	Cyber piracy (Software piracy: music and film downloading)	
9.	Hacking/ carding/cracking	
10.	Identity theft	
11.	Privacy violation	
12.	Using another user's password	
13.	Disseminating fake news	



<b>14.</b>	Plagiarism	
<b>15.</b>	Copyright violation	

(e) Others please specify

.....  
.....  
.....

(f) The following is a list of cyber technologies. Please kindly (tick (√) any or all that you use and are familiar with.

Computer or Laptop	
Smartphones, Tablet	
Internet (World-wide web)	
Other	

(g) Please indicate your level of agreement with the following items or statements as applicable elements of cyber technology behaviour awareness.

**Scale: 1= Strongly Agree, 2= Agree, 3= Neutral, 4=Disagree, 5=strongly disagree**

		SA	A	N	D	SD
<b>1.</b>	I sometimes read about problems concerning unethical use of cyber technology					
<b>2.</b>	I seek guidance on the use of cyber technology in various forums on the Internet.					

3.	Cyber ethical behaviour is affected by skills and knowledge of cyber technology.					
4.	Cyber behaviour is influenced by the ability to make decisions based on prior knowledge.					
5.	I am aware of the issues and repercussions of cyber technology behaviour as a student					

### **3. Influence of attitude, subjective norm and perceived behavioural control on cyber ethical behavioural intention**

(a) Attitude toward cyber technology behaviour. Please answer YES/NO in the following table.

NO	Attitude towards cyber technology behaviour	Yes	No
1.	It is not essential to report instances of cyber ethical violations.		
2.	Learners regard incidents of cyber ethical violation as commendable behaviour.		
3.	It is tempting to engage in unethical cyber technology behaviour.		
4.	I will urge another learner to engage in immoral use of cyber technology.		

(b) Subjective norm

No.	Influence of Subjective Norm on the Use of Cyber technology	Yes	No
1.	My classmates prefer carrying out this behaviour.		
2.	My principal will want me to carry out the action.		
3.	My religious community will back me up if I indulge in cyber technology behaviour.		

4.	My family will be delighted to witness me indulge in unethical cyber technology behaviour.		
----	--	--	--

(c) Perceived behaviour

No.	Influence of PBC on Unauthorised Use of Cyber technology	Yes	No
1.	As a learner, it is quite easy for me to engage in unethical cyber behaviour		
2.	It would be relatively easy for learners at this high school to exploit cyber technology unethically.		
3.	I could easily make unethical use of cyber technology and not get caught.		
4.	My cyber technology behaviour is neither controlled nor prevented by the school's cyber technology policy.		

(d) Influence of Behavioural Intention towards Cyber technology Behaviour

No.	Influence of BI towards Cyber technology acts	Yes	No
1.	Friends and peers have an impact on a person's cyber technology behaviour, both good and bad.		
2.	The religious background of the student may influence some cyber ethical goals and behaviour.		
3.	The school's integrity has little bearing on learners' cyber technology behaviour.		

**4. Challenges of cyber ethical behaviour among high school students.**

No.	Challenges of cyber ethical behaviour among high school students	<u>Yes</u>	<u>No</u>
1.	Inappropriate use of cyber technology due to a lack of cyber morality and ethical behaviour		
2.	There is a lack of policy guidelines on how to utilise and behave appropriately online.		
3.	Appropriate understanding of cyber behaviour is extremely limited.		
4.	Inadequate security measures to ensure that cyber ethics policy is followed		
5.	Breach of network integrity and confidentiality		

(b) What challenges do you face as a high school student when using the Internet and computers

.....

.....

.....

.....

(c) Any information you want to share based on the questions above or recommendations that the school can do to improve or prevent cyberbullying.

.....

.....

.....

.....

.....

***You have reached the end of the questionnaire; your cooperation is highly appreciated.***

## APPENDIX 7: Mapping the research methodology.

### Mapping the research methodology

Paradigm/ philosophical underpinning/ worldview	Definition and attributes	Approach informed	Research designs	Sampling	Instruments
Positivism	positivism is used to study and forecast behaviour in a way that is consistent with laws; frequently used in physical and natural sciences and to some extent in the social sciences especially when a large number is involved.	Quantitative	Surveys	Probability samplings such as simple random, cluster, panel and systematic sampling	Questionnaires and content analysis

Pragmatism	In order to learn about an issue and integrate information, pragmatic thinking emphasises the critical study of facts and practical applications of the usage of diverse methods.	Mixed methods	Surveys, content analysis	Probability and non-probability sampling	Questionnaires, interviews, observations
Interpretivism/idealism/constructivism/relativism	Humans' perceptions of the world are the outcome of their mind's fabrication. People want to know more about the environment in which	Qualitative	unstructured interviews, participant observation	Non-probability sampling such as (purposive, quota, snowball, accidental and target sampling	Interviews, observations, content analysis, self-study

	they operate				
Post- positivism	The universe is limitless.	Both qualitative and quantitative	Surveys, content analysis	Probability and non- probability sampling	Questionnaires, interviews, content analysis, observations

This appendix list of identified theologies represents the far more commonly utilised paradigms in most research initiatives. According to Mphindi and Fourie, who were cited by Mthembu (2019: 56), in the fields of the Internet and telecommunications, positivism, post-positivism, and interpretivism are well-liked and frequently used research paradigms. From the range of theories listed above, positivism was selected for this study.

## GATEKEEPERS FROM SCHOOLS

### a) Empangeni High School



MNR SD ZWANE  
Private Bag x 20006 EMPANGENI,  
3880

Frank Bull Road  
TELEPHONE: 035 772 6749 FAX: 035  
792 3163  
EMAIL: [ehs12@telkomsa.net](mailto:ehs12@telkomsa.net)  
Principal:  
MR SD ZWANE

Privaatsak x 200006  
EMPANGENI 3830  
Frank Bullstraat  
TELEFOON: 035 772  
6749  
FAKS: 035 792 3163  
EPOS: [ehs12@telkomsa.net](mailto:ehs12@telkomsa.net) Hoof:

## HOËRSKOOL EMPANGENI HIGH SCHOOL

---

20 July 2022

201623159

To: Noxolo N Buthelezi

### YOUR REQUEST FOR PERMISSION TO COLLECT RESEARCH DATA AT EMPANGENI HIGH SCHOOL

- The matter above has reference.
- Empangeni high school acknowledges receipt of your letter dated 19 July 2022.
- This letter serves to be your permission to pursue your study at Empangeni high school for research purposes.
- Your study should not in any way disturb the teaching and learning activities at the school. Ensure proper arrangements are always in place with the school management.
- We wish you well in your study and hope that your findings will be shared with this office to enhance our systems in the department.

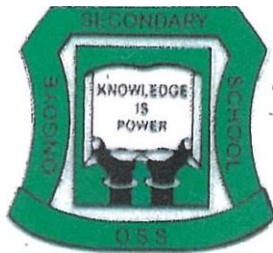
Kind regards,



SD ZWANE  
PRINCIPAL



**b) Ongoye high school**



## **ONGOYE SECONDARY SCHOOL**

No. A168 Mfundo Street, Vulindlela, KwaDlangezwa, Empangeni.  
Private Bag KwaDlangezwa 3886, Telephone, 035 7933 208/ Fax: 035 793 3208

email: [ongoyesec@gmail.com](mailto:ongoyesec@gmail.com)

Our Reference:

Your Reference:

07 MAY 2022

201623159

NOXOLO BUTHELEZI

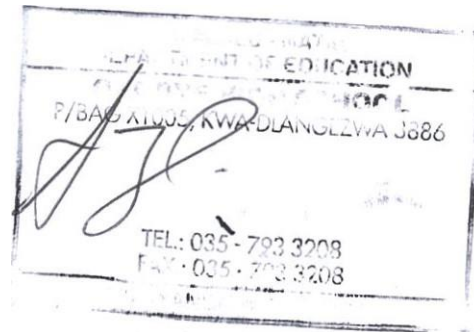
### **YOUR REQUEST FOR PERMISSION TO COLLECT RESEARCH DATA AT ONGOYE SECONDARY SCHOOL.**

- The matter above bears reference.
- Ongoye Secondary School acknowledges receipt of your letter dated 07 May 2022
- This letter serves to be your permission to pursue your study at Ongoye Secondary School for research purposes.

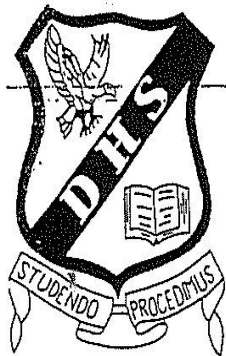
- Your study should not in any way disturb the teaching and learning activities at the school. Ensure proper arrangements in place with the school management at all times.
- We wish you well in your study and hope that your findings will be shared with this office to enhance our systems in the department.

Regards

Mrs S.J Mlenzana (Principal)



**c) Dlangezwa high school**



# Dlangezwa High School

(Est. 1969)

Private Bag X1004  
Kwa- Dlangezwa  
3886

Tel: (035) 7933615  
7933665  
Fax: (035) 7933716

09 MAY 2022

201623159

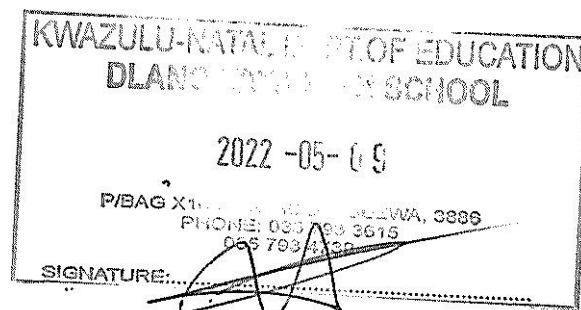
NOXOLO BUTHELEZI

YOUR REQUEST FOR PERMISSION TO COLLECT RESEARCH DATA AT DLANGEZWA HIGH SCHOOL

- The matter above bears reference.
- Ongoye Secondary School acknowledges receipt of your letter dated 07 May 2022
- This letter serves to be your permission to pursue your study at Ongoye Secondary School for research purposes.
- Your study should not in any way disturb the teaching and learning activities at the school. Ensure proper arrangements in place with the school management at all times.
- We wish you well in your study and hope that your findings will be shared with this office to enhance our systems in the department.

Regards

Mr B.V GUMEDE (Principal)



"Eagles Never Perch, But on High"

**THANK YOU!!!**