AN INVESTIGATION OF HIGH SCHOOL LEARNERS USING MXIT, AND THEIR ATTITUDES TOWARDS MOBILE SECURITY

by

Nisha Bhoola

9038406

A dissertation submitted in fulfilment of the requirements for the degree of Masters of Commerce

College of Law & Management Studies

School of Management

IT & Governance

Supervisor : Prof. M. S. Maharaj

2011

DECLARATION

I NISHA BHOOLA declare that

(i) The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.

(ii) This dissertation/thesis has not been submitted for any degree or examination at any other university.

(iii) This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced:
b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signature: NBhoola

Acknowledgements

During the course of this project, it became quite apparent to me that I could not have completed this research without the support of my family, and the continued guidance of my supervisor. I would like to specifically acknowledge the following people:-

Professor M.S Maharaj, for tolerating my many questions and queries, and especially for encouraging me through the difficult times during this project. It was through his support and supervision that I felt encouraged to complete my research. I will always be thankful for his wisdom and direction.

The principals of the schools, as well as the supporting staff, who went out their way to assist me with the handling of the questionnaires. Their co-operation is greatly appreciated.

The parents and the scholars for taking the time to complete the questionnaires.

Last but not least, my family. My children who left me undisturbed during the course of the study, and to my husband for his support, guidance and love. I would also like to thank my dad for his continuous encouragement and motivation, and to my father-in-law for his patience and support.

Thank you all. You have made this journey worthwhile.

Abstract

This research encompassed an investigation of high school learners using MXiT, and their attitudes towards mobile security guidelines. The research was conducted across thirteen schools in the Pinetown, ILembe and Umlazi districts of KwaZulu-Natal.

The literature review has shown that the majority of security guidelines and their successful use depend on education and awareness of what these security measures are. Secure use of mobile social networking sites such as MXiT are best regulated by parental awareness and monitoring of children's online habits. This needs parents to be abreast of technology, its uses and benefits, the associated dangers, as well as how to encourage and monitor usage.

The research was conducted by administering questionnaires to grades 8 to 11 inclusive in the three districts of KwaZulu-Natal. Out of the 1300 questionnaires handed out to learners, a total of 856 completed questionnaires (66%) were received and analysed.

It was found from the study that 89,5% of under age users that participated in this research are using MXiT. Users are also not fully aware of the security features when using MXiT. It has also been found that African respondents as compared with non-African respondents are less aware of the possible dangers in using MXiT, less aware that criminals can use fake IDs and pretend to be someone they are not, and less aware that people can get addicted to MXiT. Learners are aware of the dangers that can be associated with MXiT; however they are prepared to talk to strangers and meet new people online, thus exposing themselves to these dangers.

In conclusion, there is scope to improve the security measures for MXiT users, and there is a need to improve the levels of education around using these security features.

Table of Contents

Table of Figures vii

List of Tables ix

Chapter 1 : Introduction 1
- **1.1 Setting the Context** 1
- **1.2 Problem Statement** 4
- **1.3 Research Objectives** 6
- **1.4 Research Design and Methodology** 7
- **1.5 Conclusion** 9

Chapter 2 : Literature Review 11
- **2.1 Social Networking** 11
- **2.2 Online Social Networking** 11
- **2.3 History of Social Networking** 12
- **2.4 Mobile Social Networking** 16
- **2.5 MXiT** 18
  - **2.5.1 MXiT Security, Guidelines and Usage Rules** 19
  - **2.5.2 Benefits of MXiT** 22
  - **2.5.3 Criticism of MXiT** 23
- **2.6 Information Security** 26
- **2.7 Security Guidelines** 26
  - **2.7.1 Online social networks** 26
  - **2.7.2 Mobile Security** 28
  - **2.7.3 Mobile Social Networking Security** 30
  - **2.7.4 Attitudes and Awareness of MXiT Usage and Security** 32
- **2.8 Conclusion** 34

Chapter 3 : Research Methodology 35
- **3.1 Introduction** 35
- **3.2 The Research Method** 35
- **3.3 The Research Population** 36
  - **3.3.1 Sampling** 37
- **3.4 Data Collection Methods and Techniques** 39
  - **3.4.1 Questionnaire** 39
- **3.5 Data Analyses** 40
  - **3.5.1 Descriptive statistics** 40
  - **3.5.2 Analysis of Variance (ANOVA)** 40
  - **3.5.3 Dispersion Statistics Cross tabulations** 4141
- **3.6 Conclusion** 41

Chapter 4 : Data Analyses and Discussion 42
- **4.1 Introduction** 42
- **4.2 Reliability Analysis** 42
- **4.3 Demographic Data** 43
  - **4.3.1 Geographic Representation of Respondents** 43
  - **4.3.2 Race** 44

4.3.3 Gender 45
4.3.4 Age 46
4.4 Research Question 1 46
4.4.1 Age Restriction 46
4.4.2 Privacy 51
4.4.3 Reporting Abusive Users 54
4.4 Research Question 2 54
4.5 Research Question 3 65
4.6 Conclusions 70

Chapter 5 : Conclusions and Recommendations 73
5.1 Introduction 73
5.2 Literature Review 73
5.3 Research Design and Methodology 74
5.4 Summary of Findings for the Research Questions 75
5.4.1 Research Question 1 75
5.4.2 Research Question 2 76
5.4.3 Research Question 3 77
5.5 Proposed Further Research 78
5.6 Conclusions 79

References 80

Appendix A : Parent's Research Questionnaire 89

Appendix B : Learner's Research Questionnaire 90

Appendix C : Parental Consent 94

Appendix D : Sample of Letter Requesting Permission to do Research 95

Appendix E : Analyses of Variance 96

Appendix F : Descriptive Statistics 103

Appendix G : Dispersion Statistics Cross Tabulations 121

Appendix H : Ethical Clearance Letters 151

Table of Figures

Figure 4_1 : Geographic Representation of Respondents……..……...44

Figure 4_2 : Race Distribution of Respondents……45

Figure 4_3 : Gender Distribution of Respondents……..……..45

Figure 4_4 : Age Distribution of Respondents…….....46

Figure 4_5 : Parents S3.2 : Have you heard of what MXiT is?.....47

Figure 4_6 : Parents S3.3 : Are you aware of whether your child / children are using MXiT?.....48

Figure 4_7 : Parents S3.4: Has your child ever asked for permission to use MXiT?.....49

Figure 4_8 : Learners S14.11: Have you informed your parents that you have registered on MXIT?.....50

Figure 4_9 : Learners S14.11: Have you informed your parents that you have registered on MXIT * B1: Age group of respondent Crosstabulation…….……...…….50

Figure 4_10 : Parents S3.5.1: Age restrictions……51

Figure 4_11 : Learners S14.4 : Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details……..…… . 52

Figure 4_12 : Learners S14.3: When entering chat rooms, are you warned about keeping your personal information private…….……...52

Figure 4_13 : Learners S14.13 : Are you aware of the .rat command to report abuse on MXiT…….…… …..54

Figure 4_14 : Learners S16.1 to S16.4……..……55

Figure 4_15 : Learners S16.1: Are you aware of the possible dangers in using MXiT * B4: Respondent Ethnic Group Crosstabulation…..…56

Figure 4_16 : Learners S16.2: Are you aware that criminals can use fake IDs and pretend to be someone they are not * B4: Respondent Ethnic Group Crosstabulation……..…… ..57

Figure 4_17 : Learners S16.3: Do you know that people can get addicted to MXiT * B4: Respondent Ethnic Group Crosstabulation…… ..57

Figure 4_18 : Learners S16.4: Have you heard of examples where people have got abducted because of the contacts they have met using MXiT * B4: Respondent Ethnic Group Crosstabulation……..….58

Figure 4_19 : Learners S15.1 : The use of MXiT can be dangerous and open to abuse ….……60

Figure 4_20 : Learners S15.2: My cell phone password is kept secret at all times…….61

Figure 4_21 : Learners S15.3: My MXIT password is important to keep Confidential…….….61

Figure 4_22 : Learners S15.5: I only use MXIT to talk to people I know……..63

Figure 4_23 : Learners S15.6: I talk to strangers on MXIT……63

Figure 4_24 : Learners S15.10: I use MXiT to meet new people….……..64

Figure 4_25 : Learners S15.7: I download files from people I do not know……..64

Figure 4_26 : Learners S15.8: I send pictures to people I do not know…….65

Figure 4_ 27 : Learners S14.4: Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details……...…….66

Figure 4_28 : Learners S14.5: Have you shared your cell phone password with friends or anyone else……..……..…67

Figure 4_29 : Learners S14.6: Have you shared your MXIT pin with friends or anyone else……67

Figure 4_30 : Learners S14.7: Using MXiT, have you communicated with people you have not met and do not know…….……..68

Figure 4_31 : Learners S14.8: Have you ever opened a picture sent from somebody you do not know……..…....68

Figure 4_32 : Learners S14.9: Have you ever met anyone in person that you have met online……...69

Figure 4_33 : Learners S14.10: Have you ever considered meeting anyone in person that you have met online, and then changed your mind?.....69

List of Tables

Table 3_1 : Total Number of Learners in Each of the Districts…….36

Table 3_2 : Number of Learners Selected per Grade from Each District……..37

Table 4_1 : Relevant Questions used from the Research Questionnaires……..42

Table 4_2 : Case Processing Summary……..43

Table 4_3 : Parents B1 : Respondents Highest Qualification……48

Table 4_4 : Leaners B1: Age Group of Respondent……...50

Table 4_5 : Learners S14.1: I use MXiT Chat Rooms…….. 53

Table 4_6 : Learners S15.1: The use of MXiT can be dangerous and open to abuse……...62

Chapter 1 : Introduction

The advent of social networks using computers has allowed people with common interests to come together from across the globe. Online social networks have existed for over 30 years, (Borders 2009). Social networking has produced innovative ways for communication and sharing of information, and is used frequently by millions of people and is a part of daily life, (Boyd 2007). Online social networking has been around in numerous forms over the previous decade, for example SixDegrees, BlackPlanet, Ryze and Friendster, (Boyd 2007). The advent of social networking heralds a sea of change in the way personal data all over the world has become publicly available, and is pushing the boundary of societies and peoples' individual space. This is often open to abuse in various forms. The onset of mobile social networking has increased the use of social networking sites, and has made this more convenient and accessible. However, with increased accessibility, the risk of abuse has also been on the increase, and there have been numerous reports of this in the media such as "addiction", (Williams 2008), "cyber bullying", (Jacobs 2010), and "sexual predators", (Chetty 2010) to name a few, specifically since the onset of mobile social networking. The need for security measures in preventing abuse is therefore necessary.

1.1 Setting the Context

The present era of mobile social networking has taken the world by storm. With the level of technology and software that is now accessible, connections within mobile social networks are not restricted to simply sending text messages and one-to-one communication, but are moving to sophisticated communication mechanisms, (Harriman 2010). In largely mobile communities, it is possible for mobile phone users to form their own profiles, create and contribute in chat rooms, hold personal conversations, distribute photos and videos and share blogs. This can open up both opportunities and issues such as: (1) E-learning which allows the user to acquire or supply learning content on handheld devices such as PDAs, smart phones, and mobile phones, (Harriman 2010); (2) Privacy, whereby people make public considerable amounts of data into social networking platforms, ignorant of the risks of identity

theft, the prospect of this data becoming embarrassing to you in a few years, or other abuses of your personal data, (Waldvogel 2008). (3) Security - According to information supplied by WS24 (2011), malware and spam are on the increase on social networks such as Twitter, Myspace, Facebook and Linkedln. CEOs of companies are apprehensive that their employees' practice of social networks is posing a security risk for their company. A survey conducted by WS24 (2011) of over 500 organisations, reflects that 72% of them think social networks are a threat for their companies, with 60% of them labelling Facebook as the biggest security risk, followed by MySpace, Twitter and Linkedln, (Schroeder 2010); (4) Addiction - Addiction counsellor Steve Buys said that the compulsive use of cellular phones could be termed an addiction because it affects normal interactions with family members as well as work related functions, (Hollands 2007); (5) Exploitation by sexual predators, teenagers use social networking sites without appropriate supervision, whereby predators make contact with and chat to innocent young people, whom they manipulate, (Parker 2010); and (6) Difficulty in monitoring age restrictions whereby children are particularly at risk to the threats that social networking sites present. Even though several of these sites include age restrictions, it is very easy for children to lie about their ages in order to join, (McDowell 2009).

MXiT, a free instant messaging software application developed in South Africa, (Beger 2011), is the most popular social networking service available on mobile phones locally, (WS9 2009). MXiT was launched in 2005, and already has a registered user base of over 40 million; and over 700 million messages sent / received per day, (Wilson 2011). The application is circulated worldwide and is used by users in more than 120 countries daily, however the majority of its user base is in South Africa and Indonesia, (Vecchiatto 2009). The use of MXiT was extended by word of mouth because of its popularity, as well as comparatively low cost to sending sms text messages. The service is free to download, and messages can be sent instantaneously. MXiT permits the user to forward and accept text and multimedia messages to and from PCs that are connected to the internet as well as other phones running MXiT. As opposed to standard short message service technology, messages are sent and received via the Internet. Due to it being cheap to access and use, it has grown to be a very popular instant messaging service, particularly amongst the youth. The majority of users are in the age group 12 -17, (Vecchiatto 2009).

In addition to the accepted advantages of using social mobile networking as indicated above, there are various commercial and educational uses that have been developed. Advertisers have taken advantage of the large reach via MXiT users to place adverts using colour splash screen technology, (WS1 2009). MXiT users are exposed to these adverts every time they log-on, (WS1 2009). Banks are also using MXiT to increase their user base. Opening an account with First National Bank, for example, allows users to buy MXiT currency (moola) by direct debit from their bank accounts, (WS2 2009). There an also examples of MXiT being used for education and tutoring such as Dr Math which is a learning support service that offers students support between the hours of 14:00 and 20:00 between Sundays and Thursdays. Students can send a MXiT message with their query, and tutors are available on shift basis to answer their queries, (WS3 2008).

There are currently security measures, which exist to supervise the use of social networking sites for example MySpace and Facebook. These include technical methods such as filters and monitoring software, as well as non-technical methods such as placing the computer in a "public" area. By being aware that they are being watched and monitored, there is less risk of teens being abused using these sites. However, this is more difficult to monitor when accessed through a mobile phone, (Lenhart 2007).

Furthermore, when children get access to cell phone technology at an early age, they often get into self-taught habits without any guidelines, (Lenhart 2007). Unlike computers, there is no real software to block or track what people do on mobile phones. The need to understand the effectiveness of security frameworks and guidelines are therefore essential when looking at social network use and abuse using mobile phone technology, (Lenhart 2007). MXiT is linked to this mobile platform and also inherits these characteristics.

Youth Dynamix, a business-related research project focusing on consumer behaviour amongst the youth, performed a research study to keep track of business behaviour, product and media practices and lifestyle patterns by living standard measure (LSM), racial, age and gender groups. The study investigated a variety of elements of the

above mentioned, as well as a range of consumer goods, media, technology and telecommunications, (Thornton 2007).

The sample consisted of 1110 respondents; 900 children and 210 moms, the children's ages varied between 7-15 years. Despite the fact that the entire sample group of subjects were from urban areas, all the subjects came from different socio-economic backgrounds.

The study by Thornton (2007) recorded amongst others things:-

- There was a great difference in cell phone ownership between income groups;
- A high usage of SMS was recorded amongst all age groups, with an increase in voice services and game playing;
- Little usage of MMS and cameras;
- Children of all ages desire to the have the latest model of handset;
- Children predominantly download ringtones, logos, games, and 64% of moms are ignorant of the frequency of use of premium rated services.

However, research on the use of MXiT has been limited, (Chigona 2008). A study conducted with South African university students, which focused on uses of mobile internet, revealed that chatting was the key driving force for using mobile internet, and that MXiT was the core application used for chatting, (Chigona 2008). From a sample of school-going youth, it was reported that MXiT users are quite young, and that there is no major difference in usage where gender was concerned, (Francke 2007).

1.2 Problem Statement

There have been numerous media reports in recent years describing concerns relating to children obtaining access to harmful content via mobile phones. These have raised alarm bells and have been cause for concern to parents and in schools. Some examples and extracts of media reports are:-

- Chatsworth parents of teenagers with cellular phones are concerned over the latest controversy to the community – the MXiT "Sl*t-List" that is giving cell phone users nightmares. This follows the lists of embarrassment that have

been distributed on MXiT, identifying and shaming thousands of youth countrywide. The so-called "Sl*t_List" alleges promiscuity by the girls and young woman named, while the "B**t**d-List" tarnishes the character of boys and young men, (NA1 2010) .Teens send naked photos and are paid through their bank accounts. Little do they know what possible nefarious activities lay in store. Abductions of young girls that have originated via cell phone contacts have been reported in a number of South African cities, (NA2 2009).

- Of immense concern is that criminals make use of false identities on MXiT. The more the criminals get acquainted with their victims, the more private information the victims provide, (NA3 2008).
- Principals and teachers have reported that pupils "addicted" to MXiT no longer pay attention in class. The spokesperson for the Western Cape education department, Gert Witbooi, said principals were also blaming MXiT for poor performance among Grade 10s. "We have reports that learners are constantly glued to their phones," (NA4 2006).

It is evident from the above examples that teenagers are unwittingly being exposed to network stalkers and are opening themselves up to abuse. This problem needs to be investigated and understood, so that appropriate measures can be taken for education and prevention.

This leads to the problem statement for this research :
MXiT is amongst the fastest growing mobile social network in South Africa, (Oppeng 2011). Its cost effectiveness, together with its open un-moderated structure can lead to abuse which in turn exposes youth to exploitation of various forms.

The primary research question based on the above problem statement is:
What are the consequences of levels of awareness of youth regarding their participation in MXiT mobile social networks?

The research question may be further broken down into sub-problems as below.

Sub-problem 1

It is important to understand what security guidelines are available. Furthermore, security guidelines may exist, but it is also important to understand whether users are aware of these.

Research Question 1

Are users aware of the security guidelines that govern the use of MXiT on mobile phones?

Sub-problem 2

Even though users may be aware of security measures in place, their attitudes and behaviours towards these may determine their risk profile and whether they are open to predators and stalkers. It is not only sufficient to have these security measures, but just as important to get users to understand their use and make them effective.

Research Question 2

Are users aware, and if so, what are their attitudes and behaviours towards the possible dangers in using MXiT?

Sub-problem 3

Given that security guidelines exist, are users aware of them and given their attitudes and behaviours, are these security guidelines effective or not?

Research Question 3

Are the existing security guidelines appropriate and sufficient in protecting these users, and are they preventing abuse?

1.3 Research Objectives

This study investigates the effectiveness of current security measures that regulate the use of social networking sites accessed via mobile telephones, specifically MXiT, and

includes research into the awareness of learners, and their attitudes towards, current security guidelines.

The research objectives based on the problem statement and sub-problems are:-

- To understand what security guidelines are in place when using MXiT, and what the levels of awareness of these are by high school learners
- To understand the learner's attitudes and behaviour towards security guidelines that govern the use of mobile social networking sites such as MXiT
- To determine whether general mobile security guidelines as inherited by MXiT are working to prevent abuse.

1.4 Research Design and Methodology

The above aims and objectives have been achieved by conducting a literature survey and by speaking to experts in the field of social networks and MXIT, as well as by conducting research amongst parents and users of MXiT. The following methodologies have been used:-

1.4.1 Literature Survey

- A literature survey has been conducted to understand and assess existing security guidelines applicable to MXIT. Mobile security guidelines for social networking sites have also been surveyed to understand how these may be applicable and used on mobile phones. The survey also investigates attitudes and behaviour towards security guidelines that govern the use of mobile social networking sites such as MXiT.

1.4.2 Design of the Questionnaire

A questionnaire was drawn up to help answer questions and gain an understanding from both parents and students regarding MXiT use and awareness of security guidelines using MXiT. Information collected included:-

From Parents

- Basic questions on whether parents are aware of what MXiT is, and the dangers associated with its use

From Students

- Demographic information (Age, Grade, Gender)
- Details of habits using MXiT (who, how often, why)
- Awareness of problems associated with lack of security and potential for abuse
- Attitudes and behaviour towards security by asking specific questions on usage patterns of MXiT, and how learners perceive safety and confidentiality during use.

Random sampling was used to select the schools in the different districts, as this reduced the likelihood of bias, (Westfall 2009). Stratified clustered sampling was used across the actual number of learners registered in each of the schools for grades 8 to 11 inclusive. Cluster sampling is typically used when the researcher cannot get a complete list of the members of a population they wish to study but can get a complete list of groups or 'clusters' of the population, (Westfall 2009).

The questionnaire has been designed for a quantitative evaluation conducted using the analyses of variance; attitudes and behaviours have also been evaluated quantitatively using both descriptive and dispersion statistics.

1.4.3 Sample Selection

Schools were selected from the districts of Pinetown, Umlazi and ILembe, covering the Greater Durban area. Learners from grades 8 to 11 were selected. The sample was selected by means of a clustered systematic random sampling technique.

Notes on the above:-

- The number of schools were obtained from the Education Management Information System (EMIS) report, obtained from the Department of Basic Education

- The number of learners in each school was obtained
- The schools were selected randomly
- The respondent learners were selected using a systematic random sample
- The total number of learners sampled is greater than 700 due to rounding
- The total number of schools selected is greater than 10% of the total due to rounding

1.4.4 Data Evaluation

The data from the questionnaires have been evaluated to realise the overall objectives of the research, and were also evaluated by:-

- Race
- Gender
- Learner grade

The data is evaluated and discussed in Chapter 3.

1.4.5 Scope and Limitations of the Research

The research was dependent on:-

- Willingness of parents to provide access to their children
- Their command of the English language in filling in the questionnaires
- Completeness of the questionnaires filled in

1.5 Conclusion

MXiT offers the benefits of free instant messaging and a cheaper alternative to sms messaging. Furthermore, with the software that is now available, when users interact within mobile social networks, these interactions are not restricted to simply sending text messages and allowing interactions to occur on a one-to-one basis, but are moving to sophisticated communication mechanisms, (Flora 2009). With the advantages of this messaging system, there are also associated disadvantages and dangers, for which security systems and preventative measures are necessary. In this chapter the researcher has identified and outlined the problem to be studied and has given an overview of the methodology used. The literature review in the next chapter aims to provide an insight into the problems associated with MXiT and the security

guidelines that exist. This will form the basis for the evaluation of the research objectives and problem statements.

Chapter 2 : Literature Review

2.1 Social Networking

In order to understand the term social networking, it is important to recognise that in all walks of life, be it personal or professional, human beings aggregate to form groups based on common interests. People tend to congregate with others who have the same wants and needs, and by so doing unwittingly form a social structure or a social network. Most of us belong to these social structures in the real world, from book clubs and sports clubs, to charity organisations and community and neighbourhood forums. Individuals who have a common purpose or need form these social networks organically.

A social structure has been described as an organisation or a set of persons called "nodes" which are linked by one or more unique types of interdependency, for example "friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige", as described by Lappas (2010 p.1).

2.2 Online Social Networking

Social networks have unsurprisingly moved rapidly to the online world, thereby allowing people to connect faster than ever before, (Sway 2011). Social networking has produced innovative ways of connecting people together and sharing information, and as a result, online social networks are used on a daily basis by millions of people and has become a part of daily life, (Hazlett 2008). Common examples of social networking in practice today include Facebook and Twitter. These social networks may be accessed either from computers or from mobile devices.

It is reported by Carfi (2007) that online social networking has attracted wide notice during the years 1996 to 2006. These have taken many forms, and are created for a number of reasons. Some of the reasons that social networking has grown in popularity is that it helps people meet new people, find old friends, and to join interest

groups. Despite the differences in use of social networks, Carfi (2007) describes two concepts that are commonly used. The first is profiles, whereby each member in a network provides personal information during registration that focuses on a person and what's important and interesting about that person. It is a document that allows other users to learn more about the individual's interests, hobbies and activities. The second concept is connections, where online social networks permit individuals to form connections with others in the network. In various instances, these connections are implicit, which means that relations are never really formalized. An example of such a network on the Internet would be an individual's email address book. In other cases, the connections are explicit, and you consciously establish connections with other members, (Carfi 2007). These common features have contributed to making social networks a lively space of connected persons who share their abilities and interests.

2.3 History of Social Networking

Social media has developed into an essential part of present society, offering communities the chance to interact in different ways. Current general social networks have user bases which are greater than the population of most countries, (Knight 2011), and according to Chapman (2010) there are social solutions available to meet just about every user need. These social network sites allow users to share photos, videos, updates of status, meet new people as well as to connect with old acquaintances. This diversity of uses available caters for different needs and helps retain existing users, and continues to attract new users.

Social networking has evolved rapidly in recent times, starting with the initial Bulletin Board Systems (BBSs) which made their online appearance in the late 1970s, (O'Mahony 2010). They were hosted on personal computers and a connection was made by dialing in through the host computer's modem. The right to access the BBS was limited to only one user at any one time, (Borders 2009). While many legal BBSs existed, there were others that were involved in prohibited or criminal practices such as adult material, virus code, tips and commands for hacking and phreaking (phone hacking), with The Anarchist's Cookbook being an example of a resource

which was generally hosted on BBSs, (O'Mahony 2010). BBSs were the original example of sites permitting users to log on and network with one another, though in a much slower manner than we presently do, (Chapman 2011). Bulletin Board Systems could be found for almost every hobby and interest such as religion, politics, music and dating. These BBSs could be considered in many ways as a precursor to the modern form of the World Wide Web.

Subsequent to BBSs, "online services" such as CompuServe and Prodigy were amongst the first genuine "corporate" attempts at accessing the Internet, (Leelachand 2011). It is reported that CompuServe was the original corporation to integrate a chat program into their service, but they were accessible during nighttime hours only, (Adams 2011). CompuServe was expensive; it cost $6 per hour and long distance fees, which meant that it could run $30 per hour or more, (Leelachand 2011). Prodigy was subsequently developed and was responsible for online services being more affordable, (Adams 2011). Despite the prohibitive cost, and the limited availability, online forums played a major role in online web advancements.

From 1985 – 1999, Genie, an early online service, was created by a General Electric subsidiary (GEIS), (Adams 2011). The service was a text-based service designed to present consumers with forums, data exchange and e-mail within their system, (Leelachand 2011), and also offered services such as providing news, online shopping and games. It is reported by Weyhrich (2011) that even though Genie kept its costs competitive as compared to other bigger information service companies, the difficulty faced by Genie in the 1990s, as with other online services, was a combination of the rise of the World Wide Web and the graphic user interface, predominantly from the Macintosh and Windows 3.1 and Windows 95. Weyhrich (2011) concludes that for these reasons this type of computer use was making the standard text-based services less and less relevant.

IRC (Internet Relay Chat) was developed in 1988, and is regarded as the father of instant messaging, (Borders 2009). IRC was a form of real-time Internet text messaging formed mainly for debates in forums, as group communication; however it also permitted one-to-one communication by means of personal messaging along with

chat and date transfer, (Leelachand 2011). IRCs are, however, vulnerable to malicious users and are attractive for hackers, and this is noted by Riabinin (2008).

The advent of the next era saw the introduction of Six Degrees, founded by Andrew Weinreich, an entrepreneur and Internet executive, and was launched in 1997 and was the first modern social network, (Boyd 2007). Adams (2011) describes this program as a means to form an online social network to arrange the process of meeting people you don't know through the people you do know. In fact, this website was the first to organize significant features of social networking services together, for example user profiles, friend's lists, and personal messages. This website is no longer in use and had approximately one million members at its peak, (Borders 2009). AsianAvenue and Black Planet were created in the years subsequent to Six Degrees' launch, between 1997 and 2001, (Adams 2011). Whereas AsianAvenue is reportedly the biggest online communities for Chinese, Japanese, Korean, Vietnamese, Indians and others in the Asian and Asian American families to network, (Leelachand 2011) Black Planet is the largest online community for African-Americans, (Adams 2011). Users meet and connect with other members by chatting or posting photos and videos. These online social networking sites provide music, jobs forums, personal advertisements, photos, chatting; all adapted to the specific interests of the black community, (Boyd 2007).

A new approach to social networking was started in 1999 by LiveJournal. The social network focused on continuously updating personal blogs, and persuaded its users to follow one another's writing to generate groups and to interact, (Borders 2009). As with most blogs, users can comment on each other's journal entries thus establishing a sequence of comments. Leelachand (2011 p.1) describes this as being "the precursor to the live updates we see in social networks currently."

The early 2000s brought some major developments in social networking and social media, (Adams 2011). Friendster, founded in 2002 was the first modern, general social networking site, whose purpose was to provide a place for meeting new people that was safer than places used in daily life, as well as faster, (Borders 2009). Friendster allowed members to discover their friends, and then friends of friends, and so on to grow their networks. The website is also used for dating and allows users to

share videos, photos, comments, messages with members via profiles and networks, (Boyd 2007). A further major social network, Hi5, was created in 2003 and currently boasts over 60 million actively involved members, (O'Mahony 2010). When compared to other networks, profile privacy in Hi5 is treated in a different way as compared to other networks; a user's network comprises not only their own contacts, but also secondary contacts (friends of friends) and tertiary contacts (friends of friends of friends), (Chapman 2010). Profiles can be set by users to either be seen only by their network members or by all Hi5 users in general, (Adams 2011). "While Hi5 is not particularly popular in the U.S., it has a large user base in parts of Asia, Latin America and Central Africa", (Borders 2009 p.1).

Networking has been a core tactic for marketing and building businesses long before the internet era. LinkedIn, developed in 2003, was one of the first business-oriented social networking websites, (O'Mahony 2010). Profiles are filled in by users that serve as a resume for interaction through confidential messaging whereby members can determine inside relations, propose job candidates, trade experts and industry partners, (Leelachand 2011). Other features that have been added include groups, forums for posting questions and answers, and sophisticated profile features such as instantaneous, real-time updates, which help to support and expand one's existing network of trusted contacts, (Adams 2011). It appears that website technology and the attraction of making connections online makes social networking a smart means for businesses to broaden their word of mouth reach, expand their influence, and gain credibility.

MySpace was created in 2003, and by 2006 had developed to be the most accepted social network globally, (Borders 2009). This social website was different from other competitors whereby users could totally personalize the look of their profiles and post music and embedded videos from other websites, (Adams 2011). It was the leading social network by 2006, having over a 100 million users, until Facebook overtook MySpace in 2009. Facebook was developed in 2004 by Mark Zuckerberg, (Nickson 2009). Similar to MySpace, users create personal profiles, exchange messages, add other users as friends, post photos and videos. In addition, users may connect common interest user groups or networks organization by workplace, school, or

college, (Nielson 2009). Facebook now allows anyone to become a regular user of the website, so long as they are at least 13 years of age, (Adams 2011). It is reported that "this social networking site is used by more than 500 million people in every country on the planet, so far in 70 languages," (Collier 2011 p.3). It is further elaborated by Nielson (2009) that the factors that have contributed to Facebook's rapid growth, was an organized, simple and easy-to-use interface; its broad appeal, as it is not targeted towards any specific demographic; activity focus, being focused on connectivity a opposed to entertainment; architecture and inventive features; privacy and control over who sees their content; and large amounts of free media coverage. Due to the popularity and growth in Facebook, MySpace only topped the social network leagues into early 2008, and according to Whitworth (2011) it has allegedly lost more than 10 million users earlier this year and is now down to 63 million single users. Facebook's continued success was marked when it reached one trillion page visits in June 2011, making it the most viewed Web site in the world, as reported by (Anderson 2011).

2.4 Mobile Social Networking

There are an increasing number of ways in which we connect to social networking sites, (Boyd 2007). Mobile social networking is social networking where individuals with similar interests can connect, communicate and share content by using their mobile phones, (Boyd 2007). Mobile social networking is similar to web based social networking as it also occurs in virtual communities. All major digital technologies are headed to mobile telecoms, computers, the Internet etc, and all major media are headed to mobile - music, gaming, news, television, advertising and even money from banking to credit cards, available for use on mobile phones, (Valdecantos 2011). There are currently over 5 billion active, fully paid mobile phone subscribers, (Valdecantos 2011). It is described that "a tidal wave of new products and services for Mobile Social Networking hit the market in 2007 and 2008 but, in 2009, many were overshadowed by the growth of Facebook access by mobile subscribers", (Perey 2010 p.1).

Mobile phones are increasing the accessibility of the Internet and social networking sites. A survey by Jacobs Media and Ambition, a media research and consulting firm, found in 2010 that "400 million people access the Internet only using a personal computer, and that out of all 2 billion internet users; 625 million people are exclusively using a mobile phone to access internet content", (Schmidt 2011 p.6). In another survey conducted in South Africa by Dial Direct, (WS7 2010), which was run online to gain greater insight into South Africa's cell phone habits, reveals a number of very interesting facts on mobile internet access : 18% of the respondents said they spent more than five hours a day on their cell phones, while just over a quarter put that figure at four hours; 56% of respondents indicated that they used their cell phones for two hours every day; just over 30% of respondents indicated that email was the most important function after making calls; far fewer indicated that they used their cell phones predominantly for its camera (after making and receiving calls); a high proportion of respondents (63%) indicated that they used their cell phones for social purposes only, while 37% said they used their cell phones for both social and business purposes. When asked about whether or not they used their cell phones for social networking, 121 respondents said they did, while 90 said they did not. The vast majority of respondents indicated that they subscribed to Facebook, with 12,5% of respondents using their cell phones for Twitter, and far fewer for MXiT and banking.

Furthermore, statistics reported by WS8 (2010) for South Africa show that 44% of e-mails are sent and received via a cell phone, and that there are almost 6 times more cell phone subscribers than internet users. Nielson (2009) reports that people in the UK who are active mobile web users are more inclined to make use of a handset to access a social network and 23% of the population do so, comparative to 19% of the population in the US.

The facts above clearly show the explosion of Internet use, and especially how mobile phones and smart phones have made social networking more popular, more accessible and hence more frequently used. It is also shown by Beger (2011 p.5) that "South Africa is an important case study in the way that mobile phone access and usage has grown rapidly in recent years, showing that from 2005 to 2009, the number of South Africans owning, renting and/or having access to a mobile phone increased by 20 per cent., and the nation now sees 93 per cent mobile penetration among its total

population of 49 million", Beger (2011 p.5). It is also relevant from this that "increased access to mobile internet has already had a significant effect on South African society, with South Africa seeing the creation of predominantly mobile-based applications, referring to MXiT.

2.5 MXiT

MXiT (pronounced "mix it"), was founded in 2001 by Herman Heunis, a Stellenbosch University graduate, (Trennery 2010). MXiT is a free instant messaging application that runs on mobile phones with Wireless Application Protocol connectivity, (WS10 2011). Messages are sent and received via the Internet, and not with standard sms technology, (Chigona 2009). The application is without charge and the only running costs are data charges from cellular networks, which averages to under 2 cents a message compared to the standard sms rates of approximately 75 cents, (Streicher 2011). MXiT has satisfied the need for a free instant messaging application, both text and multimedia for computers as well as mobile phones, (WS11 2011).

MXiT is one of the most innovative mobile marketing mediums globally, being more than an instant messaging application, but a lifestyle mobile social network with the ability to deliver Music, Fashion and Banking solutions, to name but a few, (WS4 2010). In addition to these services, MXiT also offers its customers a range of premium services and products, such as themed chat rooms, games, skinz, wallpapers, music, Xchange, entertainment, ringtones, virtual dating game and artificial intelligence characters. The application is spread worldwide and used in over 120 countries on a daily basis, however the majority of users are based in South Africa and Indonesia with rapid growth in 123 other countries, (WS11 2011). There are also companies currently making use of MXiT, and include Nu Metro, Nokia, Samsung, MTN, Sasol, Outsurance, Standard Bank, FNB, Cadbury, Adidas, Quicksilver, Coke, GSK, Meltz and RedBull to name but a few as described in WS4 (2010).

MXiT continues to be successful in Africa. This is supported by Bremmen (2010) in stating that MXiT sidesteps a major barrier hindering the growth of social media in developing countries: Internet access. He further states that in the majority African

countries, poor infrastructure restricts access to electricity, phones and the Internet, making surfing the Internet an expensive luxury. Wallace Chigona, a technology professor at the University of Cape Town, believes cellular is an idyllic platform for social media in Africa, (Bremmen 2010), and that "Even cell phones that would technically struggle to support Internet connectivity would support MXit," (Bremmen 2010 p.1). A survey conducted on MXiT use reveals that the MXiT platform is close on 40 million registered users, attracts between 55000 and 60000 new registrations per day, and that everyday, over 350 million messages are sent on MXiT, (Schoneburg 2011). In South Africa, MXiT is currently the most popular social network, having an active user base of approximately 10 million, (Stelzner 2011). A study released by Fuseware and World Wide Worx reports that both MXiT as well as Facebook are leading the way in active user numbers, while the fastest growth in social networking in the past year has come from Twitter, with approximately 1,1 million users in South Africa in mid 2011, (Stelzner 2011). Stelzner (2011 p.1) further reports that "One of the drivers of growth of Twitter is the media obsession with the network." Most radio and television presenters with large audiences are involved in intensive drives to encourage their listeners and viewers to both Twitter and Facebook, with the former coming off a very low base. Whereas Twitter is seeing the greatest growth amongst Facebook, Twitter and MXiT, MXiT still has the highest user base in South Africa.

2.5.1 MXiT Security, Guidelines and Usage Rules

The use of MXiT is open to anyone who has access to a mobile phone that is WAP-enabled. Adults and children of all ages alike have access to MXiT, even though this is not legal for children who are not yet 14 years old. The secure use of MXiT is largely left to individuals; and for children this is left to them and their parent's approval. It is described in WS13 (2009) that MXiT does however have a number of features, guidelines and tips in place to protect minors and inform their parents about safe MXiT use. These include i) Comprehensive online security tips; ii) Discussion forum rules that forbid pornography, harassment, stalking, or any other types of abuse; iii) General rules of conduct to protect the privacy of users; iv) Full disclosure of consumer protection data; v) Improved chat room security; vi) A service where

abuse or illegal use may be reported; vii) Peer evaluation and prohibiting of repeat offenders using chat rooms; viii) Online support and assistance to users; ix) Secure access via username and password logon; x) Providing users control over profiles and unrestricted information; and xi) Restricting access to users of at least 14 years of age.

Upon registration on MXiT, a user enters their phone number and chooses a personal pin number and nickname and selects "Accept". A user cannot get a request to chat on a one-on-one basis on MXiT because the individual who you may wish to chat to, has to consent to your request, (Thomas 2007). This is one of the levels of security and privacy protection because those random strangers are prevented from exploiting the system. An alternative now exists to encrypt user-to-user messages. The encryption is executed by means of a shared password. When logging in, the password is also encrypted. A further encryption option allows services to communicate with a client using encrypted communication, (Toit 2011).

In WS12 (2011), the following additional guidelines that are part of the security features of the MXiT application are highlighted : A user must be at least 14 years old in order to use the services of MXiT; and a user who is between the ages of 14 and 17 must inform their parents of their use of MXiT services. It is further described in WS12 (2011) that privacy on MXiT instant messaging service and chat rooms are maintained by collecting personal information collected about the user in order to activate the MXiT application. Information such as your cellular telephone number, where you live, your Internet Protocol address as well as your history of using the MXiT application and services are collected. This information is also used to develop the services as well as the MXiT application, and to gather statistics on how the services are utilized. However, even though a fair amount of caution is taken to protect the user's privacy, MXiT cannot guarantee privacy. The user understands and agrees that if interaction over the Internet is not encrypted, the information that is shared is not safe. Therefore the user must agree that MXiT will not be held responsible if an unauthorised user has access to their communications. The statements above make it apparent that that MXiT leaves the onus of security and privacy to the user. Guidelines are issued, and there are also disclaimers where it is stated that MXiT cannot guarantee your privacy.

The MXiT social networking chat rooms also have additional rules and guidelines highlighted in WS12 (2011) in the interest of security and privacy. It is made clear that even though MXiT chat rooms are unrestricted, you will remain unidentified as a user. Any personal information, for instance your phone number, MXiT pin, physical home address or name of your school or any private information about your family and friends must always remain confidential and not be shared by the user. All other users of MXiT in the chat room should also be anonymous. The user's individual profile on the MXiT forum should remain confidential. Information such as telephone numbers, e-mail addresses or pictures of users must not be shared. When using MXiT, users are always advised to communicate with people they know, and to never get together physically with any strangers they have met and interacted with online. Furthermore, when using MXiT, a user is not allowed to send pictures through chat rooms, in order to protect their identity.

MXiT has also included a feature to be able to make a complaint on abusive users. There is a .rat command that enables you to 'rat' on another person if they're being offensive or abusive, (WS9 2011). This works by allowing you to rat on a particular individual once within a 20-day period. You are further permitted to rat on multiple people - however you can't just keep on ratting on the same individual. When a particular individual has 20 or more users rat on them within a 20-day period they will be suspended from using that particular chat zone for 10 days. Because your "rat" is applicable for 20 days, when that individual comes back, they may still have „points against them'. This means that if the person continues to be abusive, then they could get suspended again. Moreover, if a user has been suspended 5 times, then they will not be permitted to use the chat zone again

Furthermore, guidelines have also been issued if users have broken the rules listed. An example of this is that it is stressed in WS12 (2011) not to physically meet with contacts that you have made in chat rooms; however if you do, you are advised to adhere to some guidelines, such as : Notify someone about your whereabouts, with whom you are meeting and when you will be back; Agree to meet the contact in a public place; Ask a friend to accompany you; Make sure that your mobile phone is fully charged so that you can make a call in an emergency; Ensure that a friend contacts you after a period of time to ensure that all is well; Under no circumstances

should you call a stranger into your home or go to their home. It may be deduced from these statements that users may choose to accept the advice and guidelines posted by MXiT, or choose not to. This would depend on a number of factors which are covered in this research, such as age, gender, race group and cultural background, and the role of parents.

There is also advice to parents, to think about how to protect their children when using MXiT. MXiT is just one of the many social networks in which children can participate, and it is important that parents be encouraged to take precautionary measures. In addition to the measures mentioned previously, parents are advised to know who their child interacts with when using MXiT as well as the different chat rooms that they frequently visit. Parents are also encouraged to have discussions with their child openly about their child's online activities, and caution them on the dangers of chatting to people they don't know.

The use of MXiT is governed by South African law, (Freeman 2006). According to Freeman (2006), The Electronic Communications and Transactions Act 25 of 2000 states that service providers, for example MXiT, are not responsible for what the message contains or the misuse of the technology by users and others. Furthermore, the Provisions of the Regulation of Interception of Communications Act 70 of 2002 states that MXiT is not permitted to observe or interrupt user communications unless allowed to do so by a court order. In the chat room case of Tsichlas v Touchline Media, the judge said the following: "If discussion forum operators were required to monitor all postings for defamatory content, it would severely restrict the operation of the forum and would furthermore grossly curtail free speech", (Freeman 2006 p.4). Further duties and rights of MXiT and its users are detailed in the MXiT terms and conditions available from the MXiT website.

2.5.2 Benefits of MXiT

When users chat on MXiT, it is the individual's choice to chat anonymously. It is possible that people prefer that what they say online not to be linked with their offline identities. These individuals therefore use assumed names or even communicate

anonymously as opposed to using their true names. One of the reasons as to why people choose to communicate anonymously as stated by WS14 (2010) is that they can be free to communicate without any consequences, as sometimes criticisms, for example, are not easy to state explicitly to their boss, or to a school principal. Furthermore, the internet is now a platform for people to meet and contribute to discussions and support victims of "violence, cancer patients, AIDS sufferers, child abuse and spousal abuse survivors", (WS15 2009 p.1). These individuals are able to use various services available on the internet for example "newsgroups, web sites, chat rooms, message boards, and other services to share sensitive and personal information anonymously without fear of embarrassment or harm", (WS14 2010 p.1). Although there is alleged abuse and miss-use of MXiT, there are also significant benefits: i) It is cost effective; ii) It is protected and more confidential than SMS, email or instant messaging; iii) Enables Constitutional rights including free speech and the right to information; iv) Prepares users for real life issues by encouraging open-mindedness for various ideas and opinion; v) Allows users to discover and relate with other users who share common interests; vi) Individuals who cannot afford the costs of a computer, formal Internet or email access costs, now have access to Internet services such as instant messaging, (WS15 2009); and vii) "Enables access to information and advice on subjects young people may not obtain through other means such as AIDS information, safe sex guidelines, gay and lesbian issues, assistance with sexual abuse at home or at school, assistance with harassment at school, advice on dealing with school bullies, drug abuse assistance and advice on how to deal with racial / sexual discrimination", (WS14 2010 p.2).

2.5.3 Criticism of MXiT

South African media as well as parents of young MXiT users, accuse MXiT of allowing paedophiles to contact minor users. There have been cases of young children making friends with adults pretending to be minors and disappearing from home to meet "these friends", (Merz 2010). A 15 year old girl was allegedly drugged, then raped by a man whom she met through the popular chat forum MXiT, (Smillie 2010). In another media report, it is reported that MXiT is to blame for a teenage girl from Johannesburg disappearing for 48 hours. She apparently met someone while using

MXiT chat rooms, (Muller 2009). Furthermore, MXiT has been accused of having a lack of security in that it enables open access to pornography sites and hence permits addicts to gain access to their content of interest, (WS16 2011). A 33 year old man was accused of possessing and distributing child pornography on MXiT, (Lombard 2011).

Sixty-four percent of young South African adults say they either know somebody who has been abused, or have experienced abuse themselves, according to a survey conducted by communications company MXiT, (Manners 2009). This statistic is disconcerting as it is reflective of the intensity of abuse in South Africa. "A more alarming statistic is that 55% of the youth surveyed have not taken steps to get help or to report the crime", (Manners 2009 p.1). MXiT hosted a special "16 Days of Activism" chat room for young people to open up, realise they were not alone, and to seek help. It seems that people tend to abuse new technology to suit their own needs and wants. The youth are attracted to new technology and with this swift escalation in use, young users fall prey to predators who pretend to be friends when their true intentions were not as they seemed, (Johnson 2010). Furthermore "In the same way that criminals use the Internet to lure children, they used MXiT to make contact with young persons through public chat rooms", (Johnson 2010 p.6). As a result, the public were disturbed and angered with the technology as well as the abusers. The response from MXiT was that the developers "added additional filters and security features in order to protect their users and many parents were awakened to the importance of knowing what their children are doing on the Internet (mobile phone or PC) and how to protect them", (Johnson 2010 p.8).

There are a number of other problems teenagers have faced with MXiT as described by Thomas (2011). It can cause addiction, and people become dependent on Internet chats, and this chatting can become addictive. It has been reported by Keating (2006) that principles and teachers of some schools have reported that pupils are addicted to MXiT and do not concentrate during school lessons. These learners are frequently chatting on MXiT. Another problem is cyber bullying: "When someone is harassed, threatened or humiliated by nasty messages or pictures using e-mail, mobile phones or social networking sites, that is cyber bullying", (Sohms 2011 p.1). Dr Elsie Calitz, a psychologist explains that "The gruesome chain letters spread on MXiT among young

children are probably the handiwork of cyber bullies," (Jacobs 2010 p.1). In an incident in Secunda, a number of primary school pupils had sleepless nights after receiving a chain letter on MXiT threatening them with death, (Jacobs 2010 p.1). Children are not always warned or aware of how to block anyone who sends them offensive or cruel messages, (WS12 2011). The next problem is associated with MXiT is the existence of sexual predators: Unfortunately, sexual predators are present and are a very real threat, (WS17 2011). It is very easy for predators to search user profiles when using instant messaging and chat rooms, and can therefore discover information about probable victims since "many naïve children list personal information with no regard for safety", (WS17 2011 p.2). The existence and use of MXiT is causing concern over the safety of children, and many fear that it is a product that could lead children right into the hands of paedophiles. In a report, a sexual predator lured a 16-year old schoolgirl using MXiT and then abducted her for 5 days, (WS5 2006). In another report, a teenager was allegedly kidnapped and then raped after making contact with her attacker through MXiT, (WS6 2009).

MXiT is just a piece of technology and its control lies in the hands of the users of this technology. Its use can lead to benefits or problems. If the services of MXiT or those other instant messages were to be banned, it does not mean that the problem will go away. It is therefore important for both users and parents to be conscious of the possible dangers in order to empower themselves to use and enjoy the great benefits of the service, (WS12 2011).

In order to maintain some sense of security and control, "The Film and Publication Board (FPB) welcomes the recent announcement by the popular next generation social network, MXiT, to curb illegal activities of posting pornographic or explicit materials within its platforms," (Myeni 2010 p.1). According to Myeni (2010 p.5), "Section 24 of the Films and Publications Act holds the owners and operators of all telecommunication channels targeted at and used by children responsible for the content created and distributed within those mediums. They (owners and operators) are required to take the necessary steps in ensuring that their services are not used by any persons for committing offences on children; as evidence and real life experiences points to the fact that some of these mediums are used as platforms for sexual abuse, exploitation and grooming of children". This will no doubt encourage social network

providers such as MXiT take more precaution on safety measures for the safe use of its social network.

2.6 Information Security

"Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction", (Aceituno 2005 p.6). Wireless communication has shown great advances and as a result mobile applications and services such as instant messages, downloading contents, mobile commerce, mobile banking and information searches are becoming more and more popular, (Ying 2008). Technology advances have simplified business, enriched entertainment and made personal transactions more convenient for device users, however, it has also opened the door to security threats, (Ying 2008).

Mobile devices for example cellular phones, Personal Digital Assistants (PDA's) as well as smart phones are exposed to numerous security threats like malicious code (including virus, worm and Trojan horses), vulnerabilities of mobile phone, attacks on communication, data robbery and damage, and mobile spam, (Leem 2005). Information security is therefore a critical issue and of great concern to mobile devices users.

2.7 Security Guidelines

2.7.1 Online social networks

Online social network services such as Facebook, MySpace, LinkedIn and Hi5 have recently become accepted tools for users to share content and make it publicly available, share common interests and keep up with their friends, family as well as business associates, (WS18 2010). "A typical social network user profile features personal information (e.g. gender, birthday, family situation), a continuous stream of activity logged from actions taken on the site (such as messages sent, status updated, games played) and media content (e.g. personal photos and videos)," (Catano 2009 p.8).

The confidentiality and protection of this information is a major concern, (Gross 2005). As an example, users may upload content they wish to make available to certain friends, but do not wish this to be widely distributed to their whole network. Therefore access control and availability of the content on social network profiles is a key issue. However, this is a challenge, for example, users find specifying detailed privacy settings to be difficult and often fall short of achieving their goals, (Bonneau 2009). It is further stated by Dong (2010) that social network services have inconsistent goals. The privacy of social networking sites' client base is essential; however, to be successful, it is necessary to develop and increase the connections between their users. This is generally achieved by revealing content to users through links such as "friends-of-friends", in which content relating to persons known to a user's friends (but not the user) is revealed. Examples of this is acquiring access to a photo album of an unknown user only because a friend is tagged in one of the images, (Catano 2009). It is therefore essential for processes to be put in place for users to consistently manage access to content in online social network services. Methods also need to be implemented to enforce privacy and security policies, (Catano 2009).

There has been a significant amount of work focusing on privacy protection on online social networks, (Zhu 2010). Zhu (2010) reports that Flyby Night is a Facebook application designed to protect the privacy of messages exchanged between Facebook users. NOYB (short for "None of Your Business") is another system targeted at cryptography protecting user privacy on Facebook. A private OSN which encrypts the data of users with attribute-based-encryption (ABE) is Persona, (Zhu 2010). This encryption lets users apply policies over users who may possibly view their data. Even though some of these solutions introduced innovative techniques, a centralized server is still needed to implement and even enforce access control, which cannot protect the privacy of users against the centralized server, (Zhu 2010).

An efficient way of ensuring access control in OSN is to let users place the encrypted data on the server, and then only the users who can obtain the decryption key would decrypt and get access to the data. The benefit of this approach is that a user can post her content but those users who are unauthorized are not able to get hold of the key. However, these schemes which are based on conventional cryptographic techniques have restrictions when dealing with multiple groups of OSN since "either users must

store multiple copies of encrypted data but are unable to give data based on membership in multiple groups, or users must know the identities of everyone to whom they give access", (Zhu 2010 p.7).

To meet the privacy needs of OSN, a solution presented by Zhu (2010) offers a solution that provides the following properties: 1) Autonomy, once a user enters into a private OSN, he selects his public key and private key by himself and the OSN manager cannot get access to his private key; 2) Independence, a community is built by a set of trusted users and no third party is involved; 3) Collaboration, the kernel members can work together and collaborate to build and maintain a private OSN so as to decrease the maintenance complexity; 4) Anonymous Authentication, OSN can authenticate the validity of the user's access permission for a private OSN without a user's identity; and 5) Revocation, a community could retract the permission of approved users permanently or temporarily.

In South Africa, users of electronic communication are protected by the Electronic Communications and Transactions Act of 2002. Chapter 8 of the Act covers "Protection of Personal Information", and also has guidelines for data controllers that have access to user profiles and personal data.

2.7.2 Mobile Security

Mobile devices, for instance mobile phones, are becoming flexible devices with multiple applications and uses. These devices are used to store data in addition to running custom applications. The increased use of these devices for personal or business usage requires that access to the data stored within the device be controlled, (Perelson 2006).

A security service called Access Control, can assist in enforcing security policies for mobile users, however, this creates a need for adequate access control mechanisms to protect any stored data on the mobile device, (Perelson 2006). Mechanisms to control user access are being built into the devices and numerous high-end mobile devices

have multiple controls such as having both biometric controls and a mainstream password system, (Perelson 2006).

There is apparently no commonly adopted standard for services that control access in mobile devices, neither is there any agreement over standard access control routines in the range of mobile device operating systems, (Barker 2011). Apparently, data security on mobile devices is not of a high concern. It seems that the focus of manufacturers was on design of security routines for the communication protocols instead of for the data and applications stored on mobile devices, (Perelson 2006). Despite these efforts, over the next few years mobile attacks may exceed those against desktops, (Terry 2011). This further indicates that mobile devices have inadequate security.

Importantly, verification of a person's claimed identification through user authentication is the primary line of defence against unauthorized use of a mobile device, (WS18 2010). It is further stated in WS18 (2010 p.4) that "multiple modes of authentication increase the work factor needed to compromise a device; however, very few devices support more than one mode, usually password-based authentication." Content encryption is the second line of defence for protecting sensitive information which opens the information repository to only those individuals with the correct cryptographic key, (Jansen 2010). When a device is active, a variety of attacks can occur, therefore a third line of defence as described by Jansen (2010 p.9), is that of policy controls whereby "policy rules are enforced for all program to protect critical components from modification and limit access to security-related information". According to WS19 (2011), access control forms part of five security services, the other four services include: authentication, confidentiality, integrity and non-repudiation. The Authentication service provides services that identifies and authenticates users to the system. The Confidentiality service provides services that ensure that information is not inaccurately disclosed. In an Integrity service there needs to be a level of assurance that an unauthorized person has not altered the information in any way. Non-repudiation services ensure that the information received is from the correct source. Lastly, Access control service, associated with authorisation, either grants or rejects access to the system based on the identity of the user.

To a lesser degree there are three other security services as described by Perelson (2006). Passwords are a private value known only by authorised users in order to authenticate them. Another is Biometrics. While some of the biometric capabilities for phones would require embedded or integrated hardware such as scanners to authenticate via fingerprints, other modes of biometrics can utilize aspects already found on the phone such as the camera to authenticate via iris or face recognition or the phone itself via voice recognition, (WS20 2011). Auto Logout is a feature where the device logs the user out after a set time limit. Other related features described in Jansen (2010) are Encryption and Synchronisation. Encryption uses mechanisms to encrypt data - If the presence of sensitive information or data is unavoidable, the data should be stored in a suitable encrypted form until needed. Synchronisation allows for the backing up and restoration of data as well as the settings of a particular mobile device. These two security measures can assist to protect data in and store securely for future access.

However, not all of these features mentioned are present on all mobile devices. The one that is always available is the password control. Biometric controls such fingerprint readers are slowly becoming more common, (Deutsch 2011). Despite these features, maintaining the security of a portable device involves the active involvement of the user. Numerous built-in configuration settings and security features can often go unused. Appreciating and taking advantage of the features afforded by a mobile phone or PDA is a crucial step towards instituting a wide-ranging set of security safeguards.

2.7.3 Mobile Social Networking Security

That mobile social networks present major privacy problems is very apparent. While many of the privacy concerns originating from the web-based use of social network services are also applicable to mobile social networks, there are also a number of distinctive risks and threats against mobile social networks. Despite the solutions available to users, its success is dependent on the users understanding and attitude towards security. It is for this reason that WS22 (2010) provides safety tips as seventeen golden rules to raise awareness about the risks and threats of the improper

use of social networks, particularly when accessed through mobile devices. Some examples of this include 1) Never post sensitive information; 2) Verify all your contacts; 3) Never save your password on your mobile phone; 4) Use privacy-oriented settings. Even though these rules appear to be quite basic, it highlights that regardless of the solutions provided by mobile devices or social networks, it is up to the user to take heed and comply.

However, there are on-going attempts to improve and make mobile social networks accessed more secure. Many projects have found and offered solutions to some of these problems. Duke University's Smokescreen project, uses "cliques" amongst users which are then resolved through a trusted broker system, (Cox 2007). Assuming that users trust and know each other they are then able to "sense" each other's presence, and this scheme targeted the issue of snooping and power effectiveness on mobile devices, (Beach 2009). Peopletones let users distribute their information through shared cell tower coverage, (Li 2008). This presented a partial or fuzzy location sharing service.

According to Beach (2009), a framework for constructing context-aware mobile social networking services in a ubiquitous computing environment is called SocialAware. This system is a straightforward model for the essential components of any context-aware system, whereby the context is the user's location and personal information that must be exchanged with a central system. This framework, however, does little to safeguard the user's privacy, (Beach 2009). These systems require users to consent to access their social network profile information and at the same time associate that information with the user's identity. In the WhozThat and SocialAware systems, anyone near the mobile user can make use of a Bluetooth device to snoop on a user's shared social network ID or listen in on data sent openly over a wireless connection, as all data sent over the wireless connection is transmitted without encryption, (Beach 2009).

The spread of information and data through socially mobile users can cause serious damage. A lost or stolen cellular phone can cause important data to be lost, such as contacts, personal details, pictures and access codes, thus compromising the user's privacy, and potentially that of his contacts. Raising awareness and empowering

users on information security are the first steps in securing safety when using mobile social networks.

2.7.4 Attitudes and Awareness of MXiT Usage and Security

Even though there are security features as indicated above, the validity of these measures depends on users and their attitudes and behaviours. According to Naik (2010 p.1), van Niekerk said it was up to parents to ensure their children's safety. She further states that "Children should not be given cell phones without clear rules and information about risk. Their use should be managed and monitored. Parents should learn to use these technologies themselves and get their children to teach them if they don't know how." Contrary to this, there are other views that MXiT should force mandatory registration with minimum checks of sorts, such as a credit card or faxed identity, allowing only persons over 18 to register. This also implies that if a child wants to use MXiT, then registration should be done by the parent, as stated by a blogger on WS23 (2006).

Regarding the use of MXiT, according to Chigona (2009 p.6), “most respondents indicated that they invited and accepted invitations only from people whom they knew personally”. One respondent said: “I used to accept some of the people that I chatted with in chatrooms, but when I came to varsity I deleted all of those people and I only invite and accept invitations from people that I know. I don’t have anyone on my MXiT that I’ve never met at all. It’s like, if I don’t know their face or their surname type thing, I don’t have them on my MXiT”. Chigona (2009) further describes that some respondents indicated that some of the people they were invited by were “just friends of friends”; furthermore some users found it difficult to decline invitations from acquaintances since they “find it awkward” and consider it rude. Some indicated that they temporarily accepted invites from people they are unfamiliar with on a “trial basis”. Whether they then really become friends or not depend on their subsequent interaction.

Chigona (2009) also adds that most male users in the sample indicated that they accepted all invitations, while for the most part girls said they accepted only those

they knew and liked. This differs from Bosch (2008) when she indicated that despite the prospective sexual predators on MXiT and reports of possible abuse, girls allocated their cell phones an „independence-giving' role, allowing for safe experimentation with regard to sexual activity. Chigona (2009 p.7) also describes that most of the youth respondents chatted only on a one-to-one basis, and did not enter chatrooms. Some considered chatrooms "weird since you chat with people you don't know". One respondent said, "I don't like the whole chatroom thing; I think it's actually really stupid". Most of the negative news reports are related to chatroom activities, (WS 16 2010).

All the parents in the sample used by Chigona (2009 p.10) were anxious about their children using MXiT. Some of the concerns were related to fears that their children "may be talking to serial killers", "they are wasting time", and "they are busy with their phones instead of talking to real people". Chigona (2008) showed that parents and teachers are apprehensive about the use of MXiT amongst the youth as it is perceived to be addictive and interferes with childrens' concentration on school work. Chigona (2009 p.12) also describes that parents' negative perceptions prevented their children from using the system. It is further stated here that despite the concerns, all the parents in the sample made no endeavour to stop their children from using the system. Some parents chose to remain silent, and others chose to educate their children on "how to avoid the traps out there". Furthermore, some parents also chose not to prohibit the use of MXiT because they considered that monitoring a ban would be a challenge, as it was not easy to monitor what their children do all the time. In addition to the challenge of around the clock policing of MXiT use amongst children, the predicament parents expressed was that the cell phone was in part a necessary tool, and considered cell phones to be essential for their children since "it makes communication and coordination easier", Chigona 2009 p.13). The complexity then was how to selectively oversee the use of some of the applications on mobile phones. Significantly all the parents in the study by Chigona had spoken to their children about MXiT, and had mostly spoken about care about giving out information, and meeting people online

There is therefore clearly a difference in the attitudes of male users and female users as described above, while parents perceptions are fairly similar, believing in the cell phone as an essential tool, and not being able to monitor specific applications.

2.8 Conclusion

It has been found that the majority of security guidelines and their successful use depend on education and awareness of what these security measures are. Secure use of mobile social networking sites such as MXiT are best regulated by parental awareness and monitoring of their child's online habits. This needs awareness of parents of technology, its uses and benefits, the associated dangers, as well as how to encourage and monitor usage of such networks.

Some of the MXiT security features that have been described in this chapter include detailed online safety tips, discussion forum regulations that prohibit pornography, stalking, harassment or other forms of abuse, and general rules to protect the private information of users; full disclosure of consumer protection data, enhanced chat room security, a facility to report abuse or illegal use, peer rating and exclusion of repeat offenders from chat rooms, online support and user assistance, secure username and password logon, user control over profiles and public information, and "limiting" use to users older than 13 via parental permission.

The next chapter describes the research methodology that has been employed in exploring some of the above-mentioned security measures.

Chapter 3 : Research Methodology

3.1 Introduction

This chapter describes the research methodology applied in the study, including the method of data collection, data collection instruments, the research population and the method of sampling techniques used. The Merriam Webster Dictionary lays down the meaning of research as an "Investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws", and describes Methodology as "The analysis of the principles or procedures of inquiry in a particular field". This research methodology is the way we conduct our research and the methods we employ to improve our knowledge in any field. The research methodology links the research problems and explains the relationship between the research questions, methods of data collection, sampling techniques and collecting of data, and analyses of the research.

This study was to a large extent exploratory as the aim of the researcher was to gain an overall understanding of the use of MXiT amongst high school learners and their attitudes towards mobile security. The data collected from questionnaires was evaluated quantitatively, to understand differences between age, race, and gender. Quantitative data analyses enable data to be organised, summarised, and makes exploratory analyses possible, (Keller 2000). It also helps understand where responses are similar, or where differences exist. It is therefore applicable to this research to help understand differences between age, race and gender of learners.

3.2 The Research Method

The research sample comprises high schools in 3 districts of KwaZulu-Natal, namely the districts of Umlazi, ILembe and Pinetown. The total number of high schools in this area is 464, with 155 in the Umlazi area, 161 in Pinetown, and 148 in ILembe.

3.3 The Research Population

The target population for the study were school going children, and senior secondary learners were selected as the research population, as the majority of MXiT users are high school learners, (Bosch 2008). The sampling frame included all schools, both public and private, listed with the Department of Higher Education in the Greater Durban Area. The subjects of the study were parents, and learners from grades 8, 9, 10 and 11 from high schools in the districts of Pinetown, Umlazi and ILembe. However one school, Westham Secondary from the Pinetown district refused to participate. The number of schools in these districts was obtained from the Education Management Information System (EMIS) report of 2009, obtained from the Department of Basic Education.

The total numbers of learners in each of these districts is shown in Table 3_1.

Table 3_1 : Total Number of Learners in Each of the Districts

	Grade 8	Grade 9	Grade 10	Grade 11	Totals
Umlazi	33,671	25,919	25,839	27,308	112,737
Pinetown	33,023	24,752	25,969	26,506	110,250
Illembe	15,141	12,570	12,846	12,051	52,608
Totals	81,835	63,241	64,654	65,865	275,595

The following criteria were used to select the sample:

- A total of 15 schools have been selected, with 6 each from Umlazi and Pinetown, and 3 from ILembe, selected using random sampling.
- A total of 1500 learners were selected as a reasonable sample size, with the number of learners from each grade and district shown in Table 3_2 below. Grade 12 learners were not involved in the study as they were involved in assessments during the time of the study.

Table 3_2 : Number of Learners Selected per Grade from Each District

	Grade 8	Grade 9	Grade 10	Grade 11	Totals
Umlazi	184	141	141	149	615
Pinetown	180	135	141	144	600
Illembe	82	68	70	65	285
Totals	446	344	352	358	1,500

- The number of learners in each district was selected as a proportion of total learners in that district, thereby arriving at 615 learners for Umlazi as an example, as shown the Table 3_2 above.
- The number of learners in each grade per district was selected as a proportion of the total number of learners in that district, thereby arriving at 184 Grade 8 learners in Umlazi, as shown in Table 3_2 above.

3.3.1 Sampling

The following sampling techniques were used :-

Stratified sampling

Random sampling

Stratified Clustered Sampling

The first basis for stratification was across the actual number of learners registered in each of the schools for grades 8 to 11 inclusive from the 2009 EMIS data. A 10% sample of schools was selected as a reasonable sample size. The proportion of the total number of learners in each district as a fraction of the total number of learners was used to select the proportion of schools selected from each district, for example, there are 112,737 learners across grades 8 to 11 from the Umlazi district, with a total population of 275,595 learners across all three districts. The proportion of these learners from Umlazi is used to calculate the proportion of schools from Umlazi to be selected. This is shown in the calculation below.

$$\frac{112{,}737}{275{,}595} \times 155 \text{ schools} \times 10\% = 6 \text{ schools}$$

Similarly, the total number of schools using this method of sampling selected for Pinetown and ILembe is 6 and 3 respectively, giving a total number of 15 schools for the sampling.

Random Sampling

The random function was used to randomly select schools from a list on Excel, obtained from the Education Management Information System (EMIS) report of 2009, from the Department of Basic Education.

A manageable number of 1500 learners were selected across all the random 15 schools selected, and for convenience it was decided to select 100 learners from each school. The breakdown of learners selected by grade and district is shown in Table 3_2. A 40% (conservative estimate) response rate will give a total of 600 learners.

Of the 15 schools that were selected, one school from the Pinetown district did not give permission to conduct the research. This school was therefore excluded from the study, and a total of 1400 questionnaires were given to the remaining fourteen schools. Furthermore, one school from the ILembe district did not distribute the questionnaires to the parents or learners, and therefore no research was conducted at this school.

Out of the resulting 1300 questionnaires handed out to learners, a total of 856 completed questionnaires (66%) were received. The higher than expected response rate is due to co-ordination of the survey and involvement by teachers who played an active role in ensuring that questionnaires were completed. This could be due to "most educators working with middle and high school students are aware of the explosive involvement of youth on social networking sites," (Willard 2007). Learners' parents also had to sign a letter of consent granting them permission to participate in the survey. This was a requirement of the Ethical Clearance Committee when dealing with minors. Out of the 856 parents that granted consent, a total of 751 parents themselves completed the parent's questionnaire, and 105 parents chose to give consent but not fill in the parent's questionnaire.

3.4 Data Collection Methods and Techniques

The data collection procedure used was a self-administered questionnaire, due to the large sample size selected. Letters requesting permission to conduct research was sent to the Principals of each of the schools in each of the districts in Jan 2010. Once permission was granted to conduct research, consent forms were sent to parents, together with the parent's questionnaires. Learners that were given consent were then allowed to participate in the self-administered questionnaire, and this was co-ordinated by educators in each of the schools.

3.4.1 Questionnaire

Two types of questionnaires were developed, one for the parents and one for the learners. The questionnaires were administered and co-ordinated by teachers. The questions were a combination of demographic, multiple choice answers, and rating scale types of questions. A copy of the questionnaires can be found in Appendices A and B, with the ethical clearance letter shown in Appendix H.

The Parents' Questionnaire

The parents' questionnaire was arranged in a specific format so that the researcher may gain an understanding the following:-

> Demographic Information, such as education level and ethnic group.
> Questions about Mobile Phones and MXiT, to help understand whether parents are aware of MXiT, requirements for parental consent, and the dangers that can be associated with MXiT.

Parents' awareness of MXiT and requirements for use, as well as the dangers that can be associated with MXiT, are important factors that may contribute to security and safe use of MXiT by learners.

The Learners' Questionnaire

The learners' questionnaire was designed to provide an understanding of:-

Demographic Information, such as age, gender, grade and ethnic group.
General Questions to understand the use of MXiT
Specific Questions to understand use of MXiT, and awareness, habits and attitudes towards MXiT and the available security guidelines

3.5 Data Analyses

Descriptive and dispersion analysis has been be used to analyze the data. The basic features of the data is described and interpreted. Statistical software SPSS is used for the data analyses.

3.5.1 Descriptive statistics

The measure of central tendency of the sample has been calculated namely, the mean, the median and the mode. Secondly the measure of dispersion of the sample is obtained. These measures include the standard deviation, variance and range of the sample. Other useful statistics that has been ascertained are frequency distributions of the sample in the form of tables and graphs, assessing the reliability of the scales and assessing the normal distribution of the data.

3.5.2 Analysis of Variance (ANOVA)

An ANOVA provides a statistical test of whether or not the means of several groups are all equal. For this reason, ANOVAs are useful in comparing two, three or more means. In this study, ANOVA has been used to understand differences within District Groups, as well as Age of learners.

3.5.3 Dispersion Statistics Cross tabulations

Cross tabulations are tables of data that present results of the total group of respondents as well as results from sub-groups, and enables the examination of relationships within the data that might not be easily identifiable when analyzing the total response. Cross tabulations offer an effective way to dig deeper into research results and compare variables.

3.6 Conclusion

The methods described in this chapter were used for obtaining findings of this study, which constitute chapter 4 of this research.

Chapter 4 : Data Analyses and Discussion

4.1 Introduction

In this chapter the data from the research study is analysed and discussed. These analyses provide an understanding of the consequences of youth awareness levels of their participation and use of MXiT. This has been analysed in detail looking at each of the 3 research questions, by comparing data collected from learners and parents. The specific questions from the learners and parents questionnaires used for each research question is shown in Table 4_1 below.

Table 4_1 : Relevant Questions used from the Research Questionnaires

	Parent's Questionnaire	Learner's Questionnaire
Research Question 1	3.2 - 3.4, 3.5.1	14.3, 14.4, 14.11, 14.13
Research Question 2		15.1 - 15.3, 15.5 - 15.8, 15.10 16.1 - 16.4
Research Question 3		14.3 - 14.10

As was indicated in Chapter 3, the data was gathered through stratified clustered random sampling of schools in the Umlazi, ILembe and Pinetown districts of KwaZulu Natal. The questionnaire was distributed to 1300 scholars across grades 8 to 11 inclusive. Questionnaires were also distributed to the respondents' parents. As stated in Chapter 3, the data has been analysed by using SPSS, with both descriptive and inferential statistics being conducted.

4.2 Reliability Analysis

Cronbach's alpha is a coefficient of reliability and is commonly used as a measure of internal consistency. Cronbach's alpha is an index of reliability associated with the variation accounted for by the true score of the "underlying construct, where construct is the hypothetical variable that is being measured," (Reynaldo 1999 p.10).

Alpha coefficient ranges in value from 0 to 1 and may be used to describe the reliability of factors extracted from dichotomous (that is, questions with two possible answers) and/or multi-point formatted questionnaires or scales (i.e., rating scale: 1 = poor, 5 = excellent). As the score increases, the reliability increases. If the Cronbach Alpha value is between 0.4 and 0.7 inclusive, it indicates medium internal consistency and reliability; if Cronbach Alpha value is between 0.7 and 1.0 inclusive, it indicates a high or good internal consistency and reliability. Nunnally (1978) has indicated 0.7 to be an acceptable reliability coefficient.

Table 4_2 : Case Processing Summary

		N	%
Cases	Valid	831	97.1
	Excluded	25	2.9
	Total	856	100.0

Of the cases (users) shown in Table 4_2 above, reliability analysis of the user's questionnaire and the continuous research statements reveal the Cronbach alpha value is 0.560. It may be concluded from this that this research instrument's (questionnaire) continuous research variables have medium internal consistency and reliability.

4.3 Demographic Data

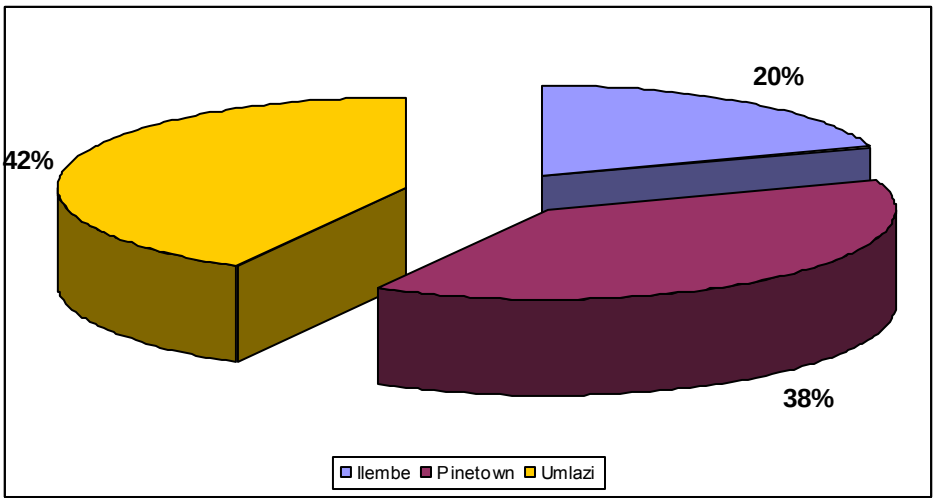
Eight hundred and fifty six respondents participated in the study. The demography of the 856 respondents in terms of gender, age and race is presented in the following subsections, with demographic details shown in Appendix F.

4.3.1 Geographic Representation of Respondents

Respondents were targeted from different geographical locations based in three districts as divided by the Department of Education namely, Umlazi District, Pinetown District, and ILembe District. The sample reflected six schools from Umlazi, six schools from Pinetown and three schools from ILembe. Figure 4_1 represents the percentage constitution of the different districts that schools of

respondents were located within. The highest number of respondents were from the Umlazi District (42,1%), followed by the Pinetown District (38,2%), and finally the ILembe District (19,7%). One of the schools selected from the Pinetown district did not participate in the research. Also, even though permission was granted for questionnaire distribution in all three schools in the ILembe district, one of the schools did not hand the questionnaires to the learners nor to the parents.

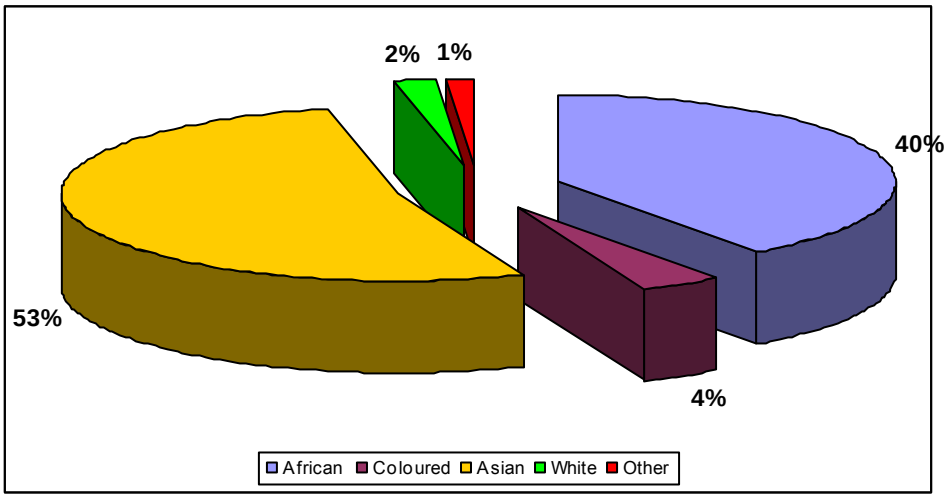
Figure 4_1 : Geographic Representation of Respondents



4.3.2 Race

Figure 4_2 describes the racial groupings of the respondents involved in completing the questionnaire. The racial distribution of learners responding to the survey, due to the random selection of schools, displays the following representation. In this respondents' race sample distribution, Asians (which consists of Indians only) consist of the largest number of respondents (52%), while African respondents are 40%.

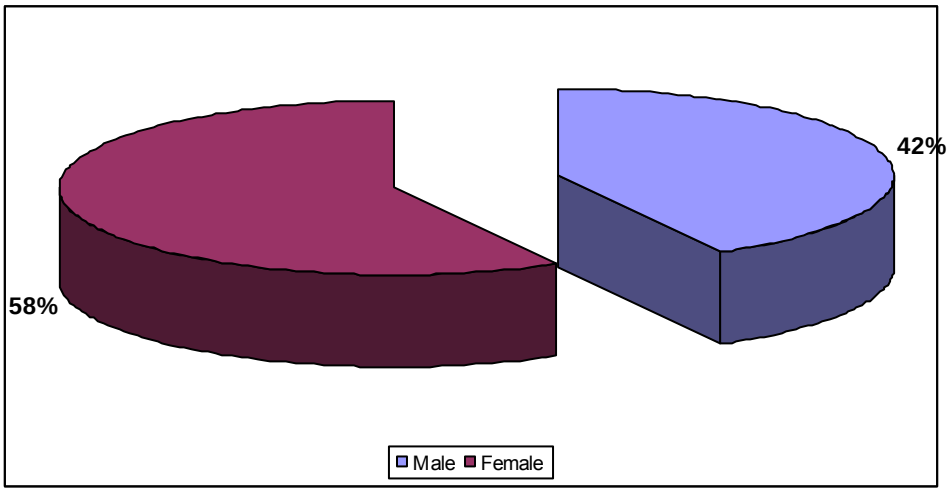
Figure 4_2 : Race Distribution of Respondents



4.3.3 Gender

The gender distribution of the respondents (as shown in Figure 4_3) are 41,9% male learners and 58,1% female learners. One of the schools was an all boy's school, and another was an all girl's school. This was not purposefully selected, and was part of the completely random selection of schools.

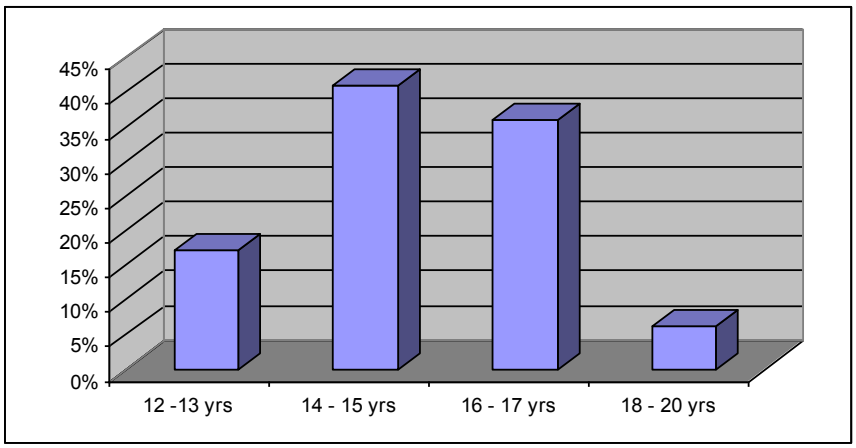
Figure 4_3 : Gender Distribution of Respondents



4.3.4 Age

The distribution of the respondents in terms of age is illustrated in Figure 4_4. This is reflective of the age distribution in grades 8 to 11 inclusive from the schools and districts selected.

Figure 4_4 : Age Distribution of Respondents



4.4 Research Question 1

In this section the research data is analysed to understand what the current security guidelines in place are that govern the use of MXiT on mobile phones, and are users aware of these security guidelines?

In Chapter 2, the current security guidelines and policies in place have been described in detail. In this chapter, we therefore focus more on whether users are aware of these security guidelines.

4.4.1 Age Restriction

One of the security guidelines in place to govern the use of MXiT is the age of the users, and is stated as follows:

"You must be at least 14 years old to enter into this agreement with MXiT. If you are 17 years and younger but older than 14 you will inform your parents/guardians that you have registered for, and are using the services of MXiT", WS 13 (2009 p.4).

In order to understand the enforcement of age restriction guidelines, it is important to test parental awareness of MXiT, and their awareness of the age restrictions applicable when using MXiT. This is relevant since all users who are younger than fourteen years should not be using MXiT, and those that are in the fourteen to seventeen year age group need their parent's permissions. Parent's understanding of MXiT and age restriction guidelines have been examined below, followed by learners understanding of these guidelines.

Figure 4_5 : Parents S3.2 : Have you heard of what MXiT is?

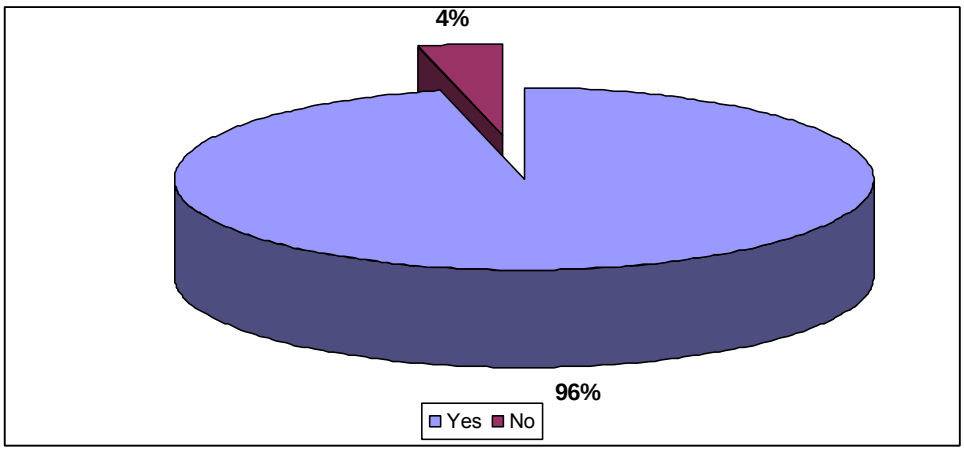
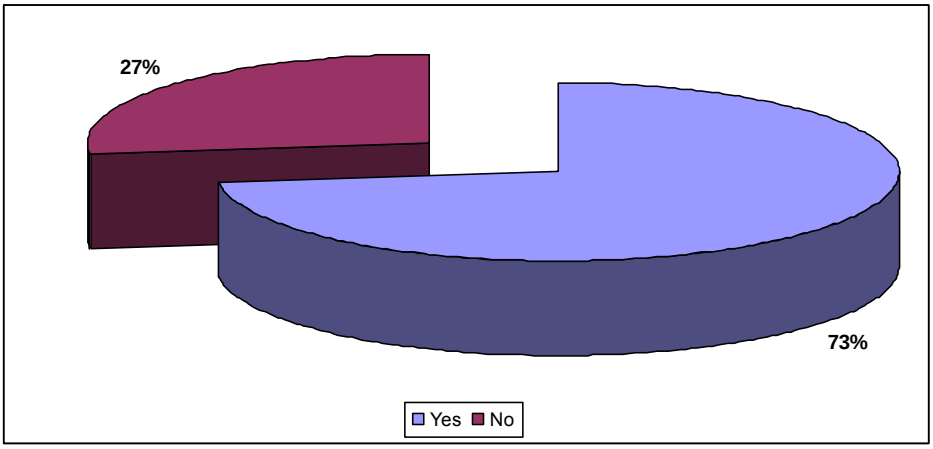


Figure 4_5 above shows that 96% of parents have heard about MXiT, and only 4% of parents have not heard about, and hence not aware of, what MXiT is. Even though 96% of parents are aware of MXiT, Figure 4_6 below shows that only 73% of parents are aware of whether their child is using MXiT, with 27% not aware. A study conducted by WS21 (2010) questioned general online use and attitudes, and shows that nearly all kids (91%) say that their parents trust them to do what's right online. However, it also shows that 56% say that their parents know some of what they do online, but not everything, and a quarter (26%) report that their parents don't have time to check up on what they do online. The results of this study on MXiT use

shows similar findings to that found by WS21 (2010), in that just over a quarter of the parents are not aware of their children's online activities, specifically MXiT.

Figure 4_6 : Parents S3.3 : Are you aware of whether your child / children are using MXiT?



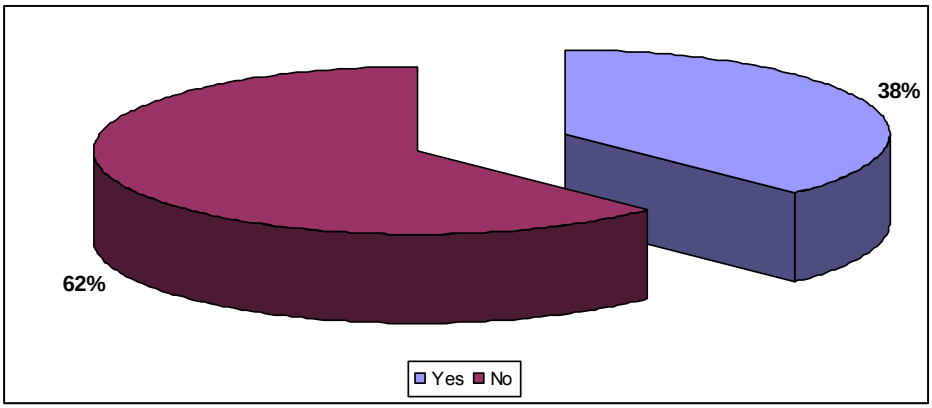
It is shown that 27% of parents are not aware of whether their child is using MXiT. This could either be attributed to a lack of parent involvement, or that parents are not aware of their children's activities on MXiT due to them not being informed. This could be attributed to the education level of parents, as we know that 32,9% of parents have lower than a matric education, as shown by Table 4_3 below.

Table 4_3 : Parents B1 : Respondents Highest Qualification

	Frequency	Percent	Valid Percent	Cumulative Percent
Tertiary	295	39.3	39.3	39.3
Matric	209	27.8	27.8	67.1
Other	247	32.9	32.9	100.0
Total	751	100.0	100	

Figure 4_7 below shows furthermore that this number drops to only 38% of parents that have been asked for permission to use MXiT, with 62% of parents not informed or asked for permission. Out of the total of 93,9% of learners who are under the age of 18, or a total of 804 out of 854 learners, only 54,7% (or a total of 440 learners) have informed their parents, with 45,3% (or a total of 364 learners) in the age groups 12-13 years, 14-15 years, and 16-17 years had NOT informed their parents.

Figure 4_7 : Parents S3.4: Has your child ever asked for permission to use MXiT?



Only 57% of learners have informed their parents that they are registered on MXiT, and 43% of learners have not informed their parents (as is shown in Figure 4.8 below). This is despite the fact that 93,9% of learners (as shown in Table 4_3) are under the age of 18 and should have at least informed their parents, or asked for permission if below the age of 14 years. Table 4_4 shows that there are 146 learners that responded who are 12-13 years of age, which represents 17,1% of the total number of learners. If the security guideline on age restriction was working effectively, it would be expected that the majority of these learners would not be using MXiT. Figure 4_8 shows that only 10,2% of these under-age learners, or 91 respondents, had informed their parents. A further 6,1%, or 55 learners, had not informed their parents. Therefore it has been calculated that 55 out of 146 learners, or 37,7% in the age group 12-13 years have NOT informed their parents that they are registered on MXiT, and they should not even be using MXiT to start with as they are under-age.

Figure 4_8 : Learners S14.11: Have you informed your parents that you have registered on MXIT?

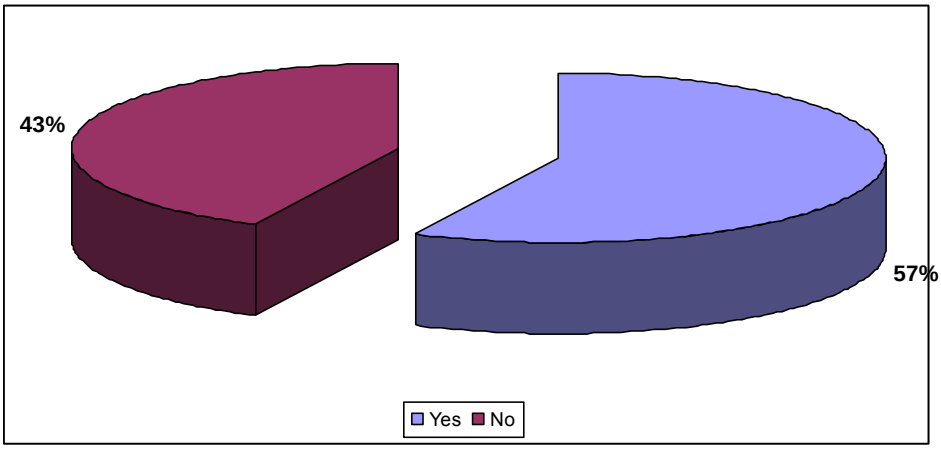
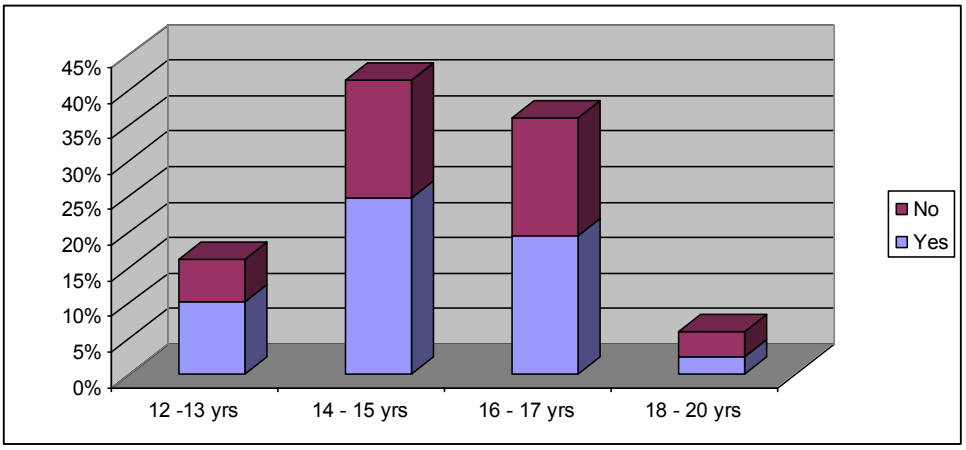


Table 4_4 : Leaners B1: Age Group of Respondent

	Frequency	Percent	Valid Percent	Cumulative Percent
12 -13 yrs	146	17.1	17.1	17.1
14 - 15 yrs	351	41.0	41.0	58.1
16 - 17 yrs	307	35.9	35.9	93.9
18 - 20 yrs	52	6.1	6.1	100
Total	856	100.0	100.0	

Figure 4_9 : Learners S14.11: Have you informed your parents that you have registered on MXIT * B1: Age group of respondent Crosstabulation

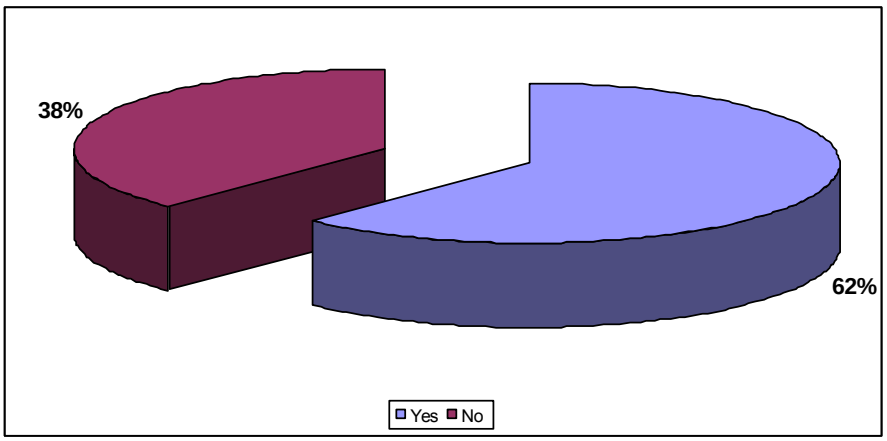


Findings in a study conducted by WS21 (2010), show that in their study of parental influence, about a third (32%) of kids say that they don't tell their parents what they are doing online, and would change their behaviour if they knew their parents were watching (31%). The study also shows that "Even though parents are less likely to

monitor their children's behaviour as they get older, young people are more inclined to hide what they do online from their parents as they get older. By the time they reach the ages of 16 or 17, 56% of teens hide their online activities", (WS21 2010 p.4).

These findings are further reinforced by the evidence shown in Figure 4_10 below, where 38% of parents are not aware of age restrictions required when using MXiT. All parents should be aware of these age restrictions as this helps monitor usage and prevent abuse of innocent and perhaps naïve children.

Figure 4_10 : Parents S3.5.1: Age restrictions



4.4.2 Privacy

The second security guideline is about maintaining privacy while using MXiT. An example of the privacy guideline is stated as follows as shown in Chapter 2 :-

> "Your personal profile on the MXiT forum should remain personal. Do not include any information that could identify you, such as your email address, phone number, home or school address or pictures of yourself", WS 13 (2009, p.11).

Figure 4_11 : Learners S14.4 : Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details

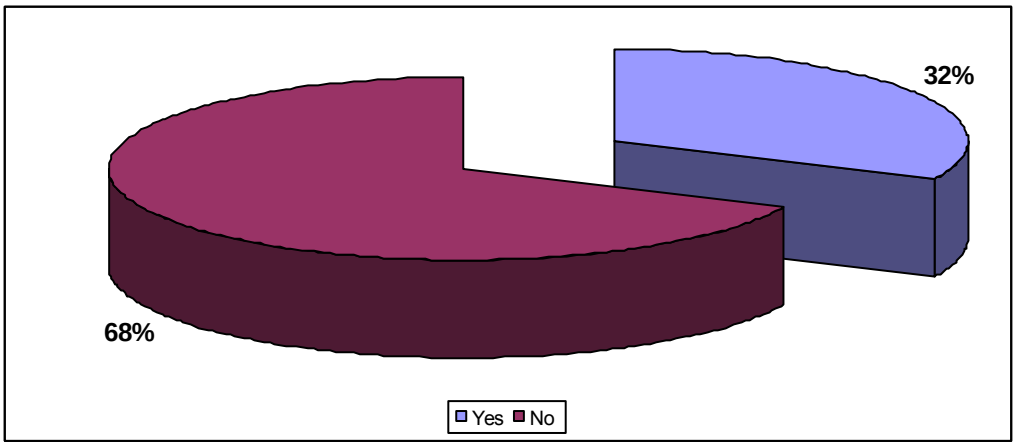


Figure 4_11 above shows that 32% of learners have indicated that they have revealed personal information on MXiT, and 68% of learners have not revealed any personal information.

Figure 4_12 also indicates that only 74% of learners are aware that they are warned of keeping their personal information private, and 26% of learners are not aware of this. This is unexpected as 31% of respondents claim to use chat rooms – this is indicated in Table 4_5. Therefore only a small proportion of respondent learners that use chat rooms are aware of this warning message.

Figure 4_12 : Learners S14.3: When entering chat rooms, are you warned about keeping your personal information private

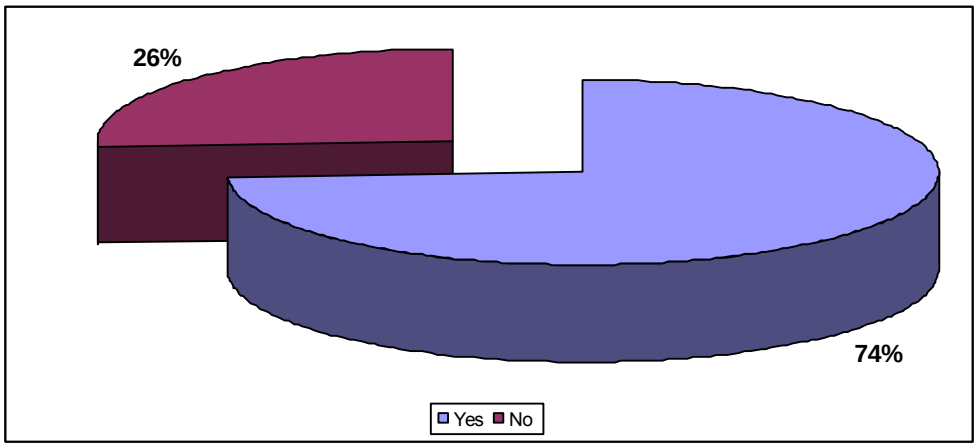


Table 4_5 : Learners S14.1: I use MXiT Chat Rooms

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	259	30.3	31.0	31.0
No	577	67.4	69.0	100.0
Total	836	97.7	100.0	
Missing	20	2.3		
Total	856	100.0		

Chat rooms are the only place that one is able to reveal personal information to strangers. Revealing personal information details in any chat room (not only a MXiT chat room) is dangerous, but teenagers and users do not always see this as a danger. MXiT ensures that users are reminded all the time not to reveal personal information. In fact, every time a user enters a chat room, the user is reminded about the dangers of revealing personal information. Teenagers also have more freedom and can make their own decisions as parents tend to lessen protection. This is supported by an interesting finding from Shallcross (2010) which shows that 71% of all parents stop monitoring their child's use of the internet after the child turns fourteen.

A survey conducted online by WS21 (2010 p.6) revealed that "despite news headlines, teens are providing more information than they should with strangers":

- 69 percent of 13-17 year olds divulged their physical location
- 51 percent of teens say they have given out personal information online to someone they don't know in the offline world
    - 43 percent have shared their first name
    - 24 percent have shared their email address
    - 18 percent have shared a personal photo of themselves
    - 12 percent have shared their phone number
- 28 percent of teens chat with people they don't know in the offline world

Tracy Mooney, McAfee's chief of cyber security states that "Kids know not to talk to strangers - it's one of the first lessons you teach them. But online, there's a sense of trust and anonymity, so kids let their guard down. Kids would never hand out their name and address to a stranger in the real world, so it's alarming to see how many kids do that very thing online", (Mooney 2011 p.3). Learners do

not see the dangers of talking to strangers online, as they would of strangers in person.

4.4.3 Reporting Abusive Users

It is stated in Chapter 2 that MXiT has also included a feature to be able to make a complaint about abusive users. There is a .rat command that enables you to 'rat' on another person if they're being abusive. The detail of how this works is described more fully in Chapter 2, and awareness of this feature is explored.

Figure 4_13 : Learners S14.13 : Are you aware of the .rat command to report abuse on MXiT

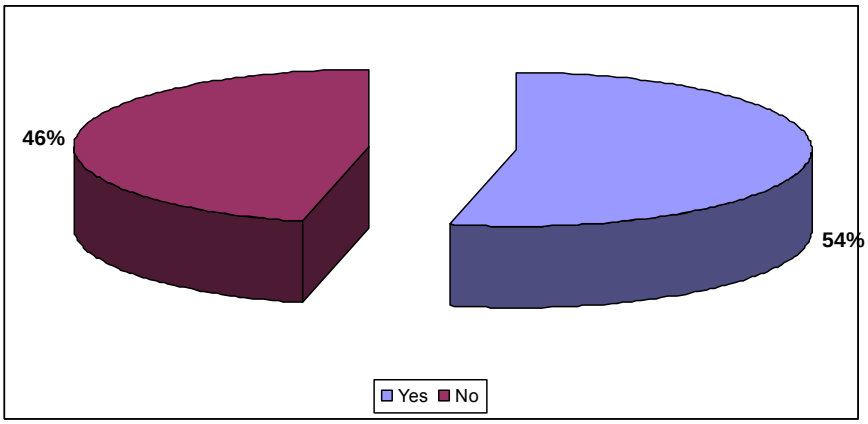


Figure 4_13 above reveals that only 54% of users are aware of this command and security feature to report abuse, and 46% of users are not aware of this. This is a high proportion of users that are not aware, by which may be concluded that this feature is not working well in helping users report and prevent abuse.

4.4 Research Question 2

In this section we use the data to analyse and understand whether users are aware of the possible dangers in using MXiT. The analysis also investigates users' attitudes to, and behaviours towards, existing security guidelines?

Figure 4_14 : Learners S16.1 to S16.4

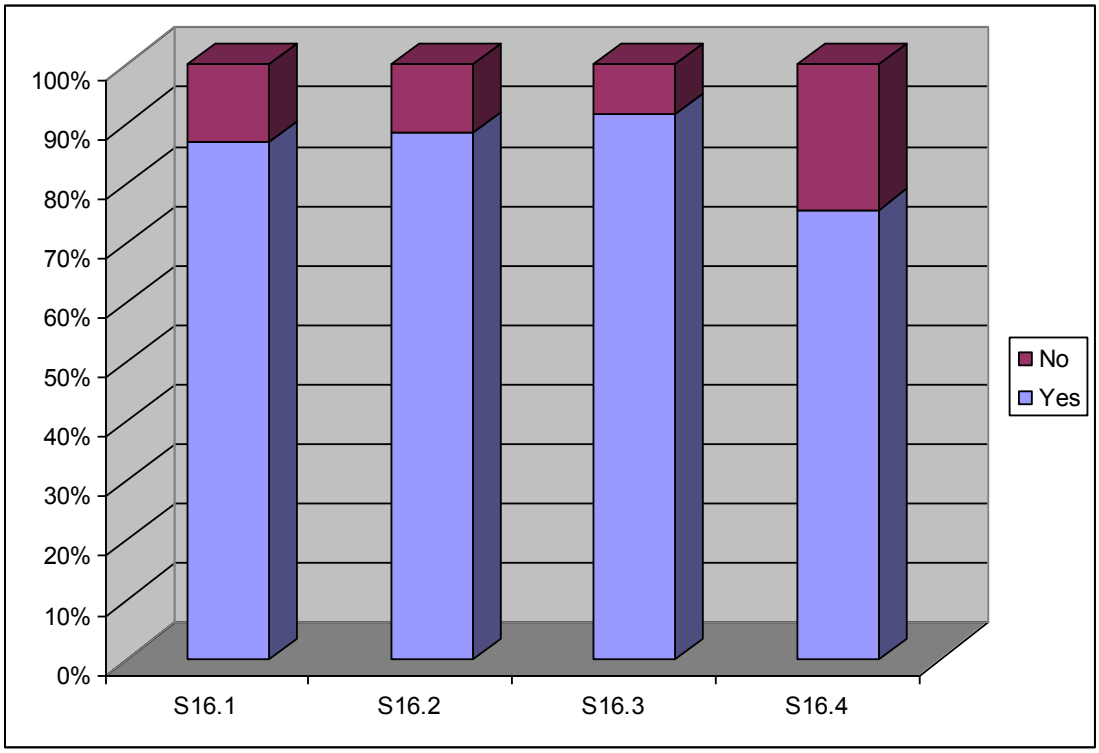
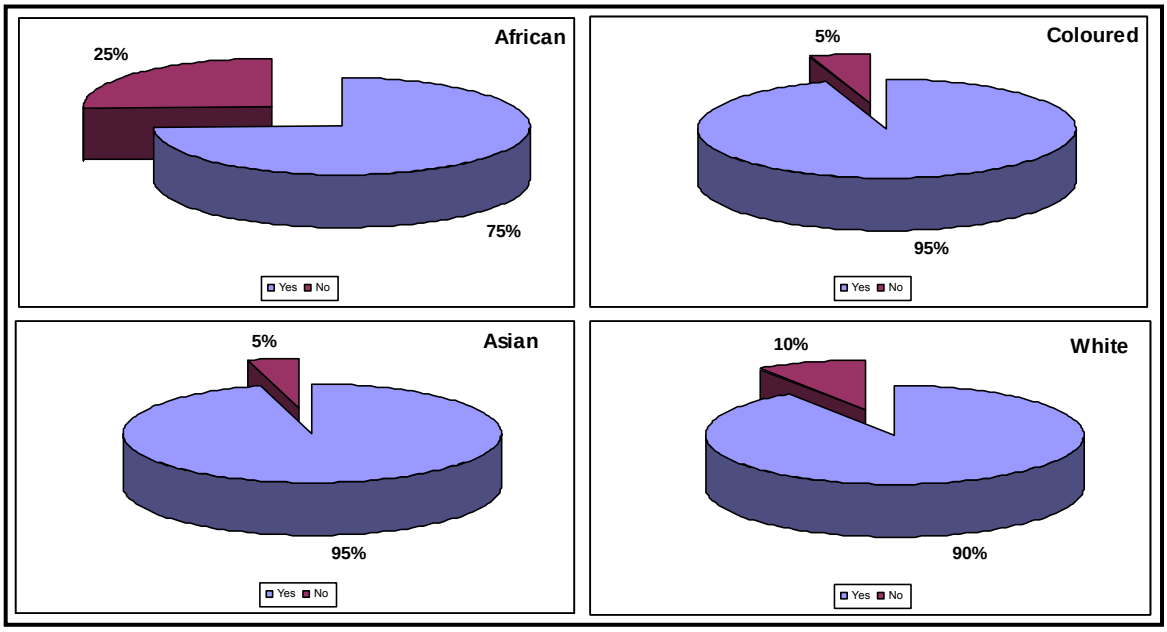


Figure 4_14 above shows that for question 16.1, 87% of users are aware of the possible dangers of using MXiT, and 13% are not aware of these dangers. In answer to question 16.2, 89% of users are aware that criminals can use fake IDs and pretend to be someone they are not. 92% of users have answered in 16.3 that they know that people can get addicted to MXiT. However, comparatively only 76% of users have heard of examples where people have got abducted because of the contacts they have met using MXiT.

Figure 4_15 : Learners S16.1: Are you aware of the possible dangers in using MXiT * B4: Respondent Ethnic Group Crosstabulation



The understanding of learners' awareness of possible dangers and abuse is broken down by ethnic group in Figure 4_15 above. There are 25% of the African learners that are not aware of the possible dangers of using MXiT, much higher than any other ethnic group. There are 5% of Coloureds, 5% of Asians, and 10% of White learners that are not aware of the possible dangers of using MXiT. It may therefore be stated that African users of MXiT among the sample group are less aware than other ethnic groups of the possible dangers in using MXiT. Incidents involving MXiT are reported by the media, and have already been discussed in Chapter 1.2. These articles help to raise awareness among users about dangers they could be exposed to and therefore support them in protecting themselves from harm.

It is also shown in Figure 4_16 that 20% of African learners are not aware that criminals can use fake IDs and pretend to be someone they are not. 22% of Coloured learners are also not aware of this. A lower percentage of Asian learners, 4% are not aware of this fact, and all White learners in the sample group are aware of criminal activity. It is therefore concluded that more African and Coloured learners are not aware that criminals can use fake IDs and pretend to be someone they are not.

Figure 4_16 : Learners S16.2: Are you aware that criminals can use fake IDs and pretend to be someone they are not * B4: Respondent Ethnic Group Crosstabulation

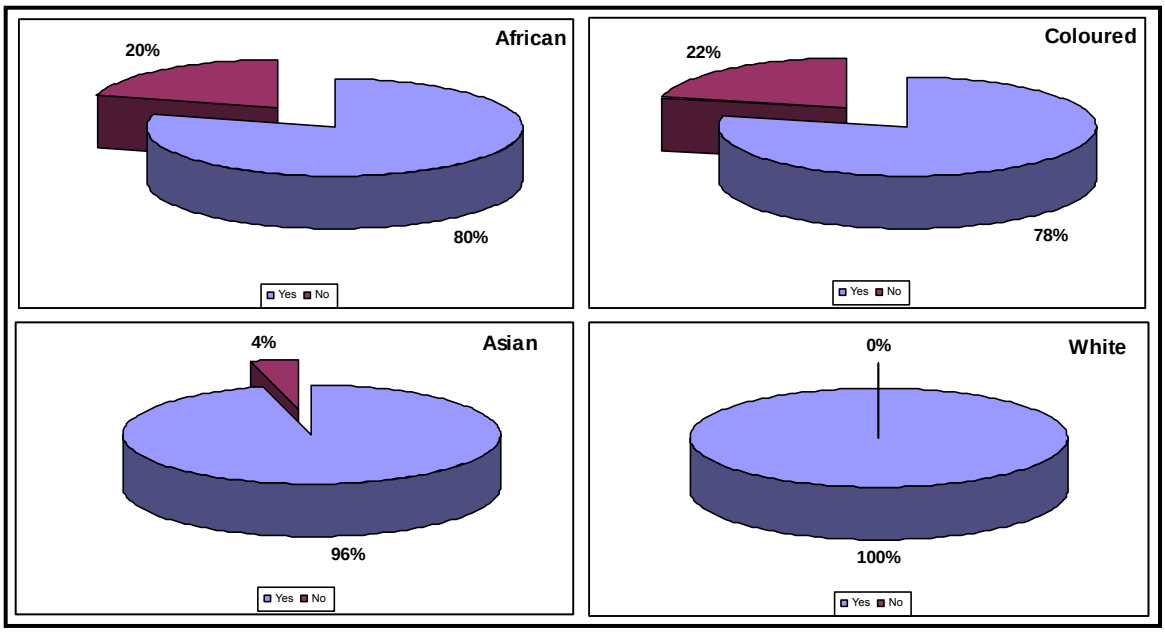
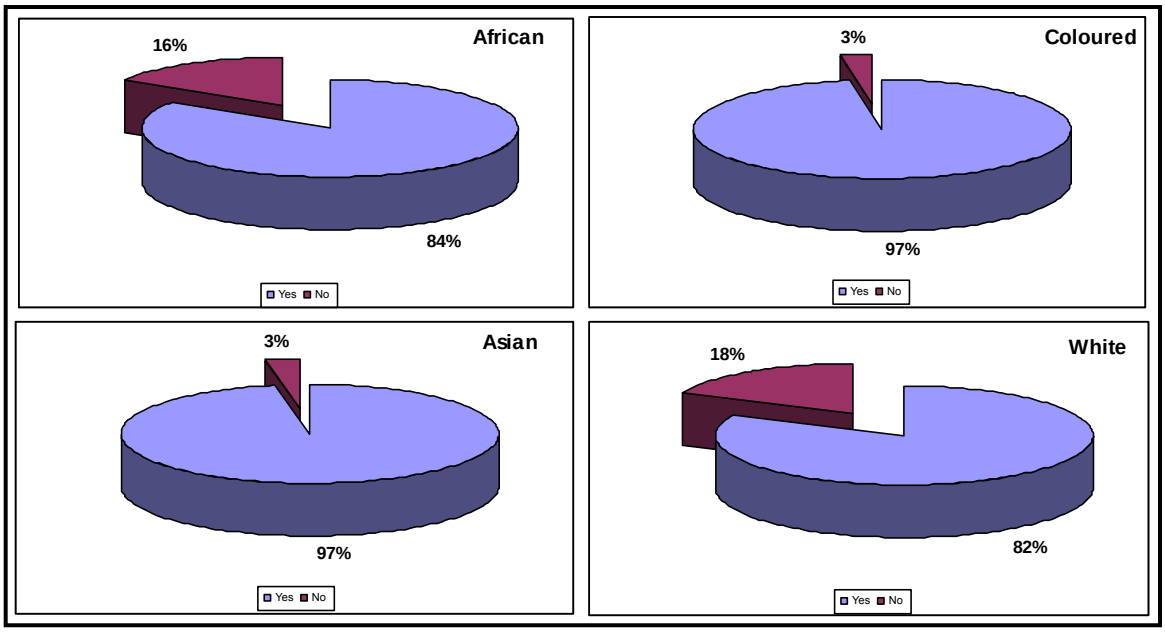


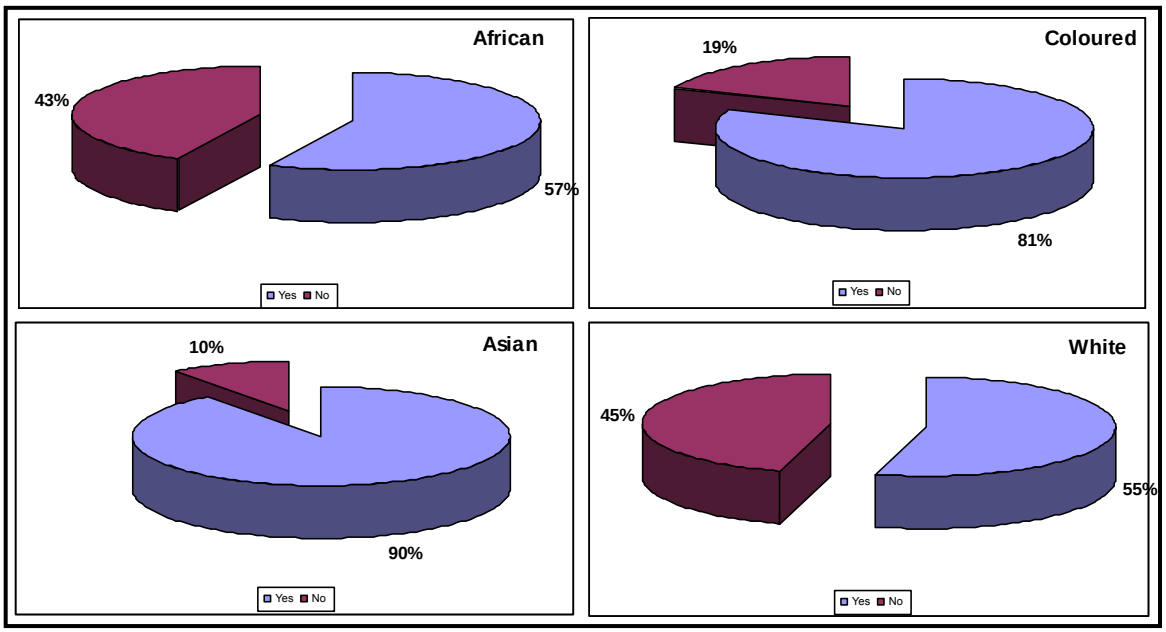
Figure 4_17 : Learners S16.3: Do you know that people can get addicted to MXiT * B4: Respondent Ethnic Group Crosstabulation



This pattern is repeated in Figure 4_17 above, showing that 16% of African learners do not know that people can get addicted to MXiT. There are only 3% each of Coloured and Asian learners that are not aware. 18% of White learners are also not

aware of this addiction; however, the total number of white learners is small at only 2,1% (or 18 our of 856 learners) of the total sample. The data therefore shows that African learners are less aware that people can get addicted to MXiT compared to the other ethnic groups.

Figure 4_18 : Learners S16.4: Have you heard of examples where people have got abducted because of the contacts they have met using MXiT * B4: Respondent Ethnic Group Crosstabulation



In Figure 4_18 above, the cross-tabulation between S16.4 and the respondent ethnic groups are shown. 43% of African learners have not heard of examples where people have got abducted because of contacts they have met using MXiT. This is higher than the proportion of Coloured and Asian people, where 19% and 10% of learners respectively have not heard of these examples. The proportion of White learners not aware of abduction through MXiT is also high at 45%; however this can be attributed to the small sample size of total White learners. It is observed from Figure 4_12 above that African learners are less aware than other ethnic groups of abduction caused through the use of MXiT. Examples of abduction cases in South Africa have been previously quoted in Chapter 2.5.3.

For the results depicted in Figures 4_15 to 4_18 inclusive, and in order to test for significant differences, it was decided to test the responses of African respondents to

non-African respondents. This is due to the relatively small number of Coloured, White and Other population groups relative to the African and Asian populations. In each of these cases, the following null hypothesis was assumed: each ethnic group has the same incidence of "yes" responses, as this would be expected in a normal distribution. The alternative hypothesis would be that the responses from the African respondents would be distinct from the responses of the non-African respondents. This was done using a 2 sample T-test; thereafter using ANOVA to test for significant differences. The results of this are shown in Appendix E. With the p values less than 0,005, it is shown that these results are significantly different between groups at the 95% confidence interval. This shows conclusively that the null hypothesis is not valid, and that the responses of the African respondents are significantly different when compared with that of the non-African respondents for these questions. More specifically:-

- 74,8% Africans are aware of the possible dangers in using MXiT, as compared to 95,0% non-Africans,
- 79,6% Africans are aware that criminals can use fake IDs and pretend to be someone they are not, as compared with 94,6% non-Africans,
- 84,1% Africans are aware that people can get addicted to MXiT, as compared with 96,6% non-Africans,
- 57,4% Africans are aware of examples where people have got abducted because of the contacts they have met using MXiT, as compared with 87,8% non-Africans.

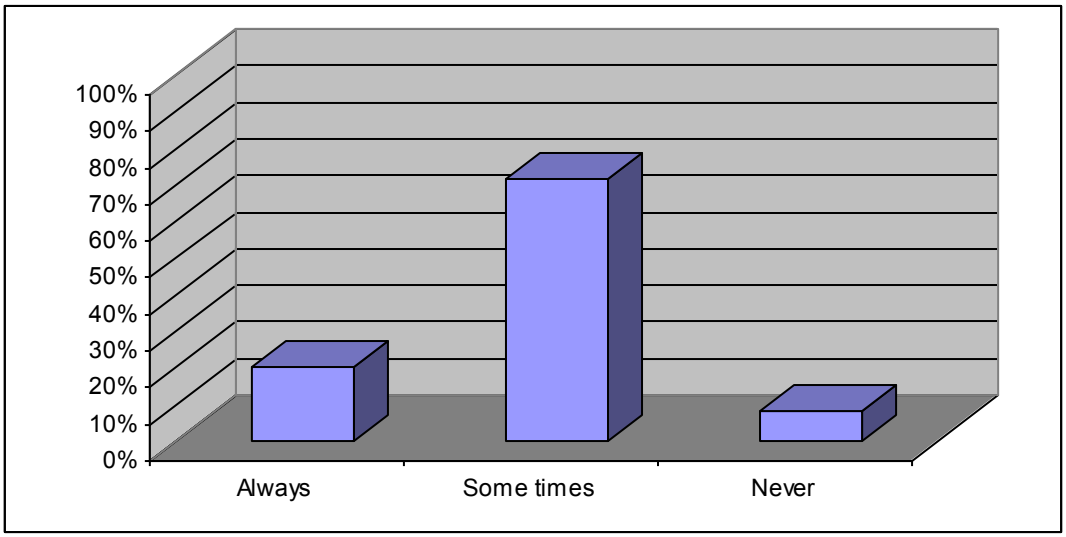
It can therefore be concluded that African respondents as compared with non-African respondents are less aware of the possible dangers in using MXiT, less aware that criminals can use fake IDs and pretend to be someone they are not, less aware that people can get addicted to MXiT, and less aware of examples where people have got abducted because of contacts they have met using MXiT.

In the following paragraphs, there were a number of questions selected to assess the research question pertaining to the attitudes and behaviours of the learners.

Figure 4_19 below shows that a total of 91,9% of learners have some awareness that MXiT can be dangerous and open to abuse, made up of 20,1% of learners that are always aware, and 71,8% of learners that are sometimes aware. Only 8,2% of learners are not aware of the dangers and possible abuses that can be associated with MXiT. The analyses of Question 15.1 in Appendix F shows that the result is not significant at the 95% confidence level between either district, grade, or age groups, with all the p values being greater than 0,05 for this question.

This is consistent with question 16.1; as previously been confirmed in Figure 4_14, 87% of learners confirm that they are aware of the possible dangers in using MXiT.

Figure 4_19 : Learners S15.1 : The use of MXiT can be dangerous and open to abuse



Password protection is fundamental in protecting one's identity and forms the basis of mobile security too. Figure 4_20 below shows that of the learner respondents that are part of this study, 76% of learners always keep their cell phone password secret, and a total of 24% either sometimes (18%) or never (6%) keep their cell phone password secret.

Figure 4_20 : Learners S15.2: My cell phone password is kept secret at all times

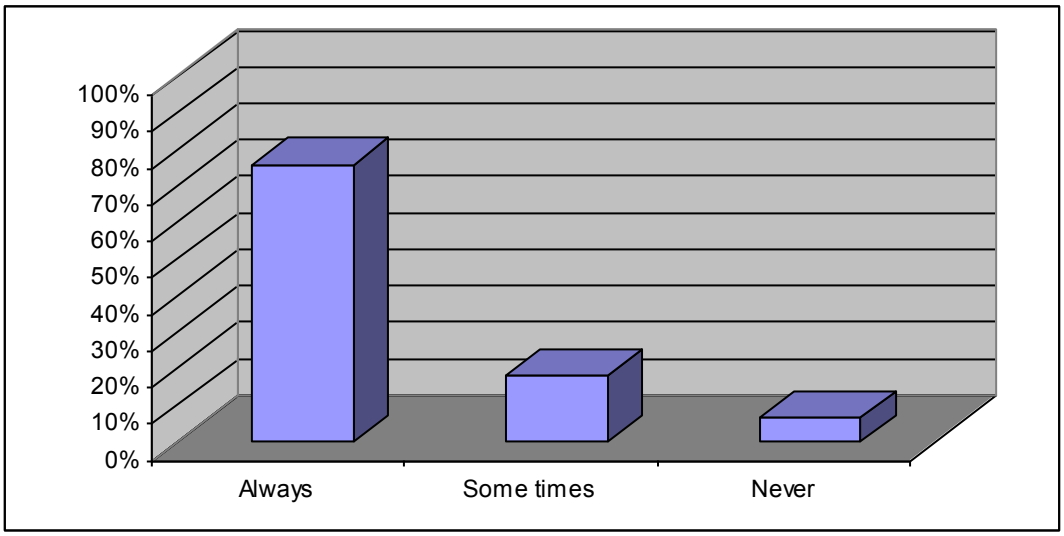
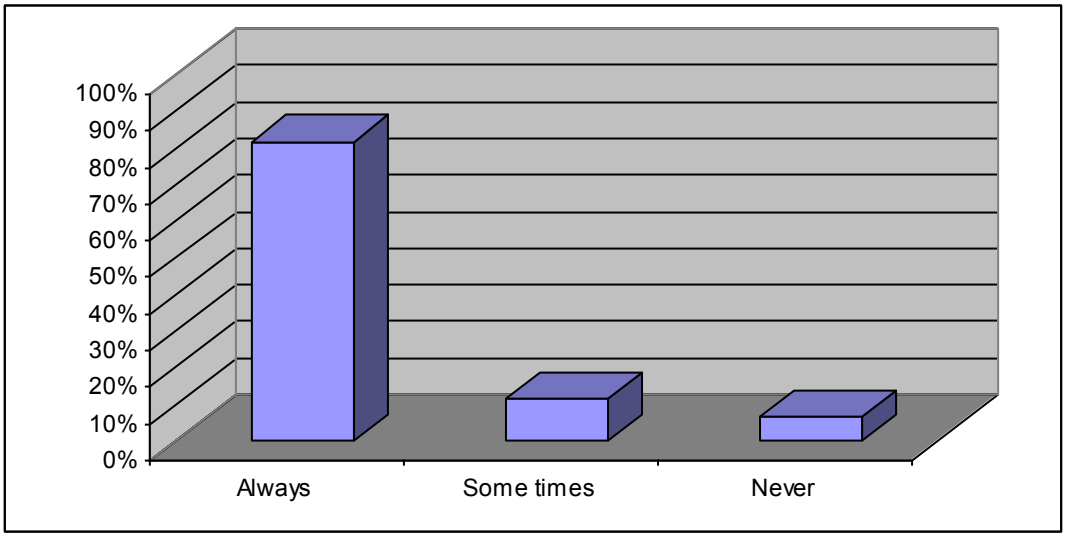


Figure 4_21 shows that a slightly higher percentage of learners (82%) state that it is important to keep their MXiT password confidential, and a total of 18% state that it is sometimes (12%) or never (7%) important to keep their MXiT password confidential.

Figure 4_21 : Learners S15.3: My MXIT password is important to keep confidential



Password protection is therefore important and used by most learners, with more than three-quarters of learners understanding the importance of confidential passwords, and treating them as such on their mobile phones.

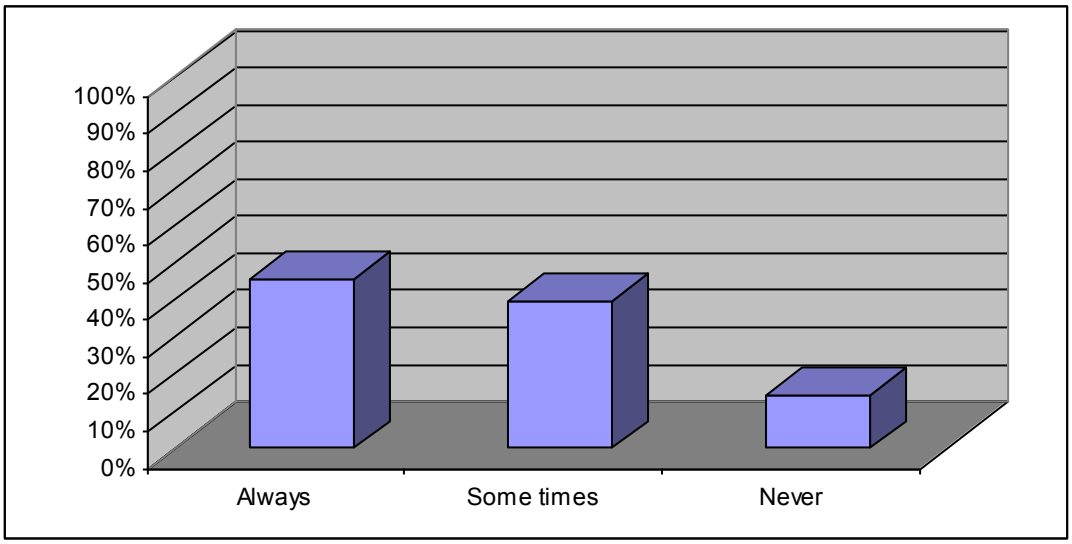
It is shown in Figure 4_22 that 45,7% of people only use MXiT to talk to people they know. A total of 54,2% of learners either sometimes or never talk to known people, which means that they sometimes or always communicate with people they do not know. This percentage of 54,2% of learners that may communicate with strangers is higher than the percentage of learners (8,2% from Table 4_6) that are not aware that MXiT can be dangerous and open to abuse. It may therefore be concluded that even though 91,9% of learners are aware of the dangers that can be associated with MXiT, more than half of the learners interviewed (54,2%) may still talk to strangers.

Table 4_6 : Learners S15.1: The use of MXiT can be dangerous and open to abuse

	Frequency	Percent	Valid Percent	Cumulative Percent
Always	167	19.5	20.1	20.1
Some times	597	69.7	71.8	91.8
Never	68	7.9	8.2	100.0
Total	832	97.2	100.0	
Missing	24	2.8		
Total	856	100.0		

It is also shown using ANOVA tests, as shown in Appendix E that this result is statistically significant at the 95% confidence level between district (p=0), between age groups (p=0) and between grades (p=0,024), as these p values are below 0,05. This means that the different district groups, age groups, and grades have significantly different perceptions towards this statement, and there is adequate difference in these different group respondent's opinions towards these statements.

Figure 4_22 : Learners S15.5: I only use MXIT to talk to people I know



Figures 4_23 and 4_24 below show similar trends as described above. 49,4% of learners (11,3% always and 38,1% sometimes), as shown in Figure 4_23 below, talk to strangers on MXiT. Similarly Figure 4_23 reveals that 62,6% of learners (21,5% always and 41,1% sometimes) use MXiT to meet new people. This is alarming considering that only 8,2% of learners (shown in Table 4_5) are not aware that MXiT can be dangerous. This data therefore supports the finding that even though learners are aware of the dangers that can be associated with MXiT, they are still prepared to strangers and meet new people online, thus exposing themselves to these dangers.

Figure 4_23 : Learners S15.6: I talk to strangers on MXIT

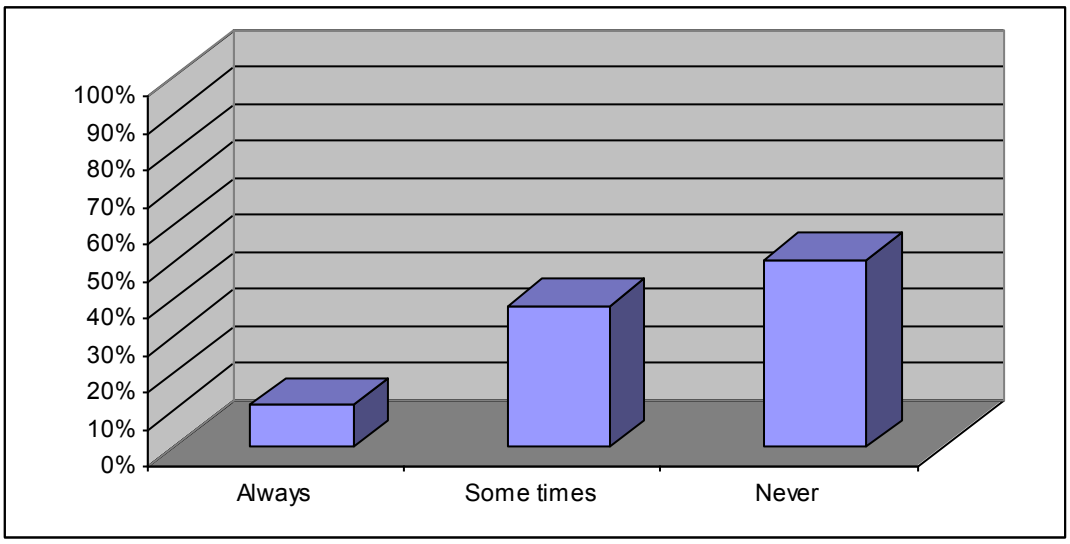
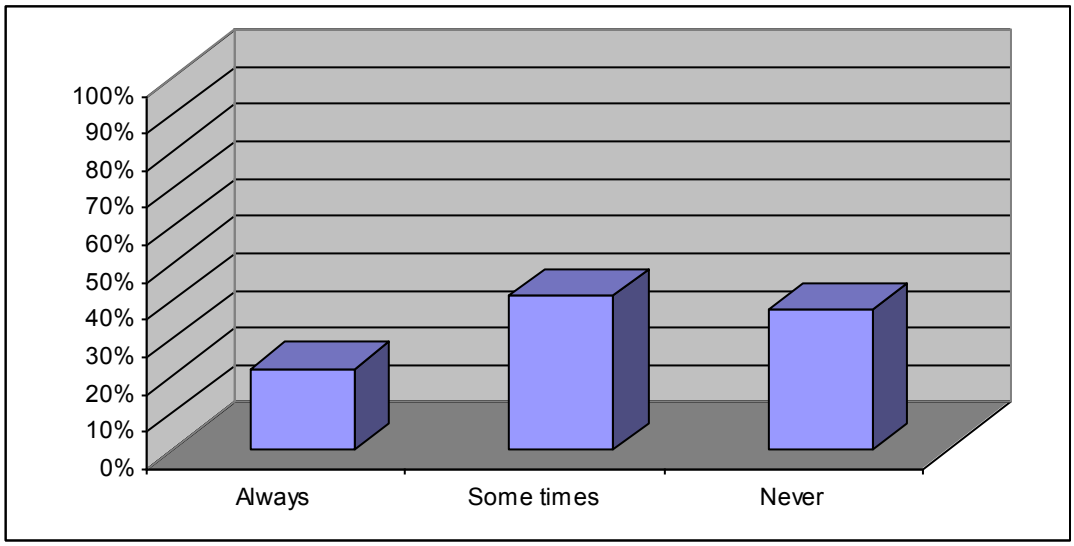


Figure 4_24 : Learners S15.10: I use MXiT to meet new people



A total of 33,6% of respondent learners always (7,6%) or sometimes (26,0%) download files from people they do not know (as shown in Figure 4_25). In addition, 22,3% of respondent learners always (4,4%) or sometimes (17,9%) send pictures to people they do not know (Figure 4_26). Even though these numbers are lower than respondents talking to strangers and meeting new people, there is still a fair proportion of people that risk their safety by communicating through sending and receiving pictures on MXiT, despite being aware that this can be dangerous.

Figure 4_25 : Learners S15.7: I download files from people I do not know

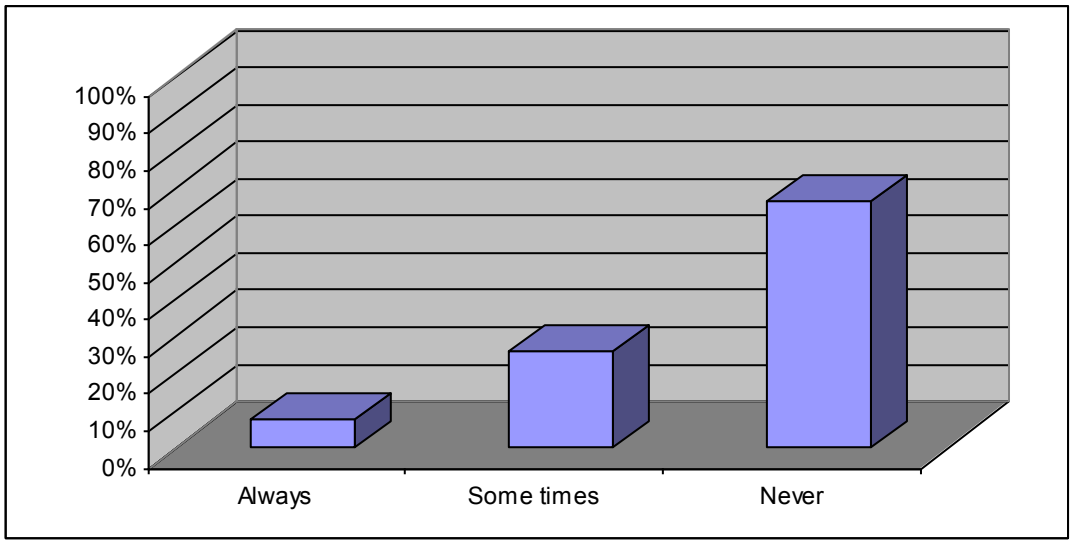
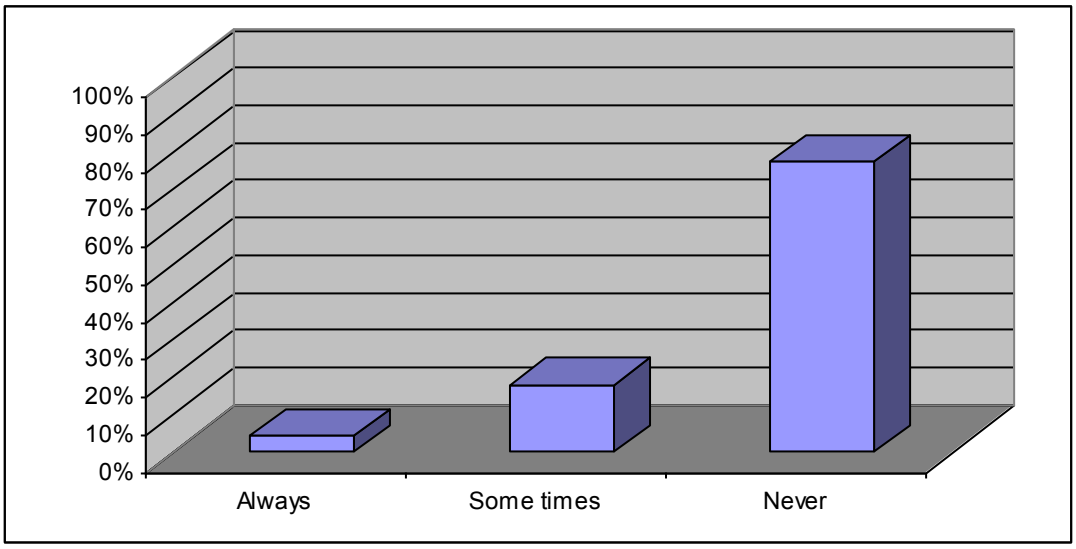


Figure 4_26 : Learners S15.8: I send pictures to people I do not know



Even though there may be abuse of MXiT, and that respondents may be aware of this abuse taking place, 39,8% of learners will not inform their parents. It is shown in Appendix E that this result is statistically significant at the 95% confidence level between age groups, with p=0 (which is below 0,05), meaning that different age groups respondents have significantly different perceptions towards this statement, with the 12-13 year olds more likely to always inform their parents.

It may be concluded that 87% of the users in this research are aware of the possible dangers in using MXiT, and these results differ by ethnic group, specifically between African and non-African users. African respondents as compared with non-African respondents are less aware of the possible dangers in using MXiT.

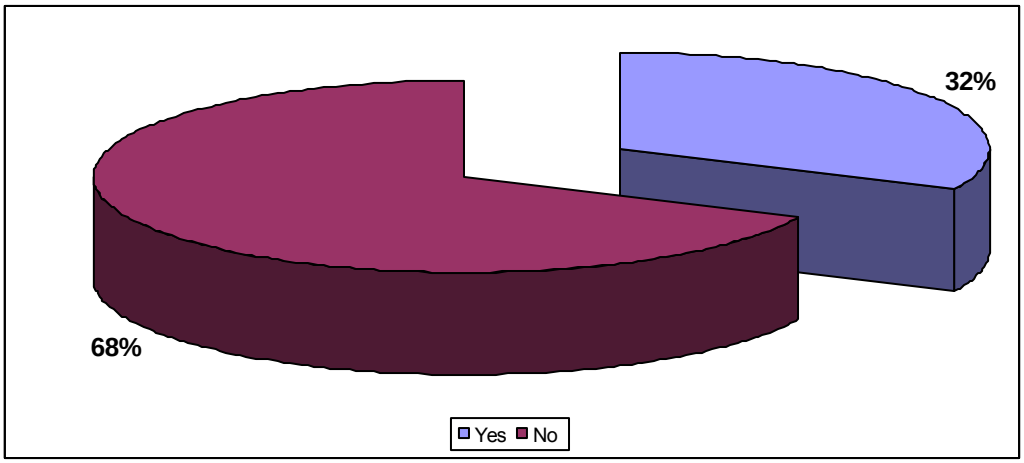
4.5 Research Question 3

This section assesses data to understand the following: Are the existing security guidelines appropriate and sufficient in protecting users, and are they preventing abuse? Given that security guidelines may exist, that users are aware of them and given their attitudes and behaviours, are these security guidelines effective or not?

In this section questions 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9 and 14.10 of the learner questionnaire will be analysed to investigate the above research question, as these sections from the learner respondent's questionnaire are most relevant.

Figure 4_27 shows that 32% of people have revealed personal information on MXiT previously, this despite the warnings not to do so. This could either show a disregard for these warning messages, and be an indication that learners believe that the dangers may not be applicable to them. This behaviour, however, may make these users susceptible to unexpected danger.

Figure 4_ 27 : Learners S14.4: Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details



Figures 4_28 and 4_29 respectively show that 19% of learner respondents have shared their cell phone passwords, and 21% of learners have shared their MXiT passwords. This is an unexpectedly high number. The basics of security and password protection should be known amongst all users, as this forms the basis for good online behaviour. However, with approximately 20% of users sharing their passwords, there is clearly a behaviour which indicates apathy towards these norms and guidelines, placing themselves at risk of being victims of security breaches.

Figure 4_28 : Learners S14.5: Have you shared your cell phone password with friends or anyone else

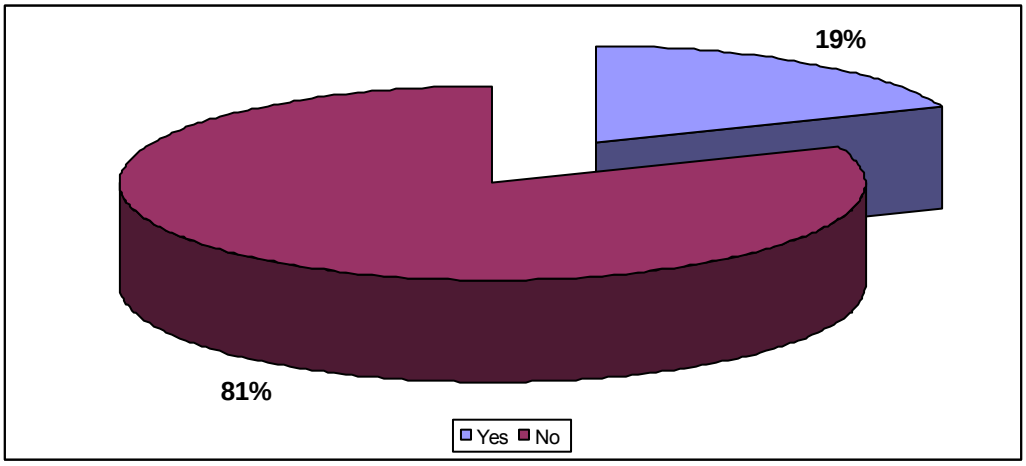
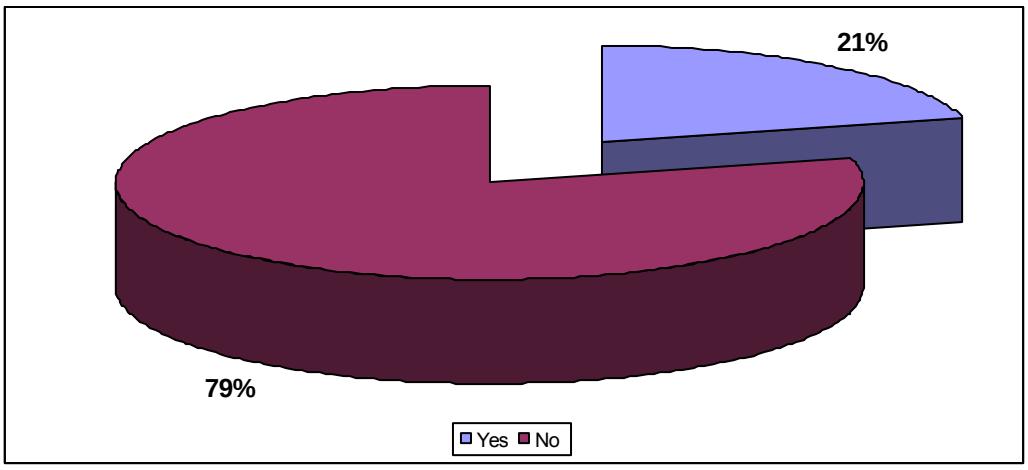
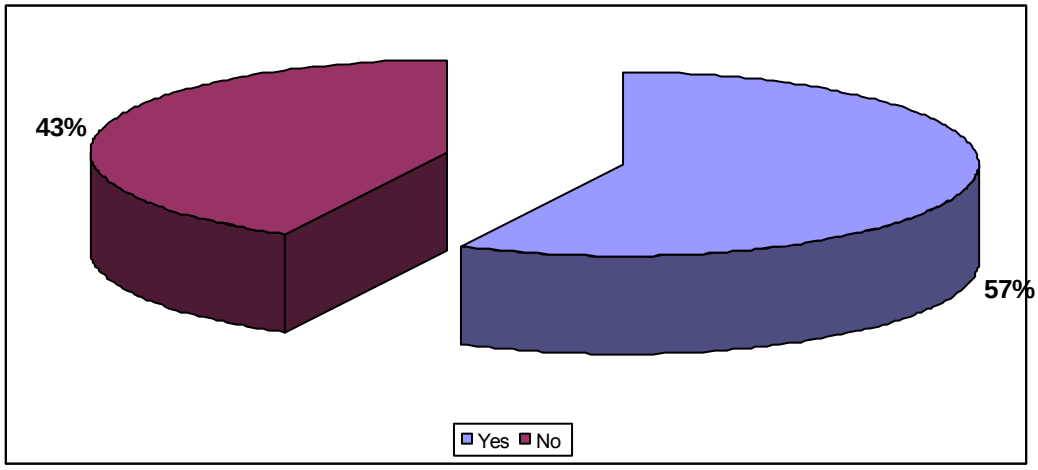


Figure 4_29 : Learners S14.6: Have you shared your MXIT pin with friends or anyone else



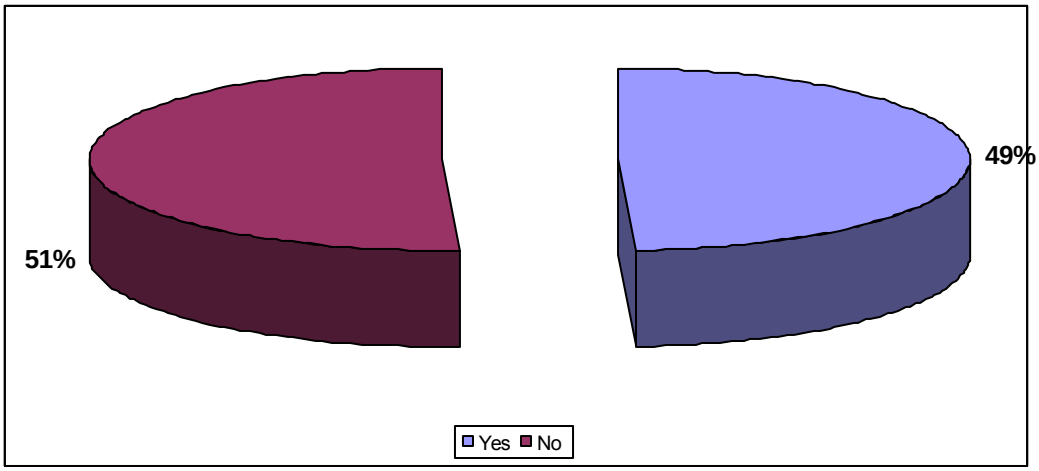
It is further shown by the evidence in Figure 4_30 below that 43% of learners have not communicated with people they have not met and do not know, while 57% of learners have. There is clearly a disregard for warning messages not to do so, and this behaviour can open one up to a sense of false security and unwittingly lead to abuse.

Figure 4_30 : Learners S14.7: Using MXiT, have you communicated with people you have not met and do not know



The data depicted in Figure 4_31 indicates that 49% of respondent learners have opened a picture sent by somebody they do not know, despite warning messages not to do so. This behaviour could be attributed to curiosity, and this curiosity could lead to unknown and anonymous danger.

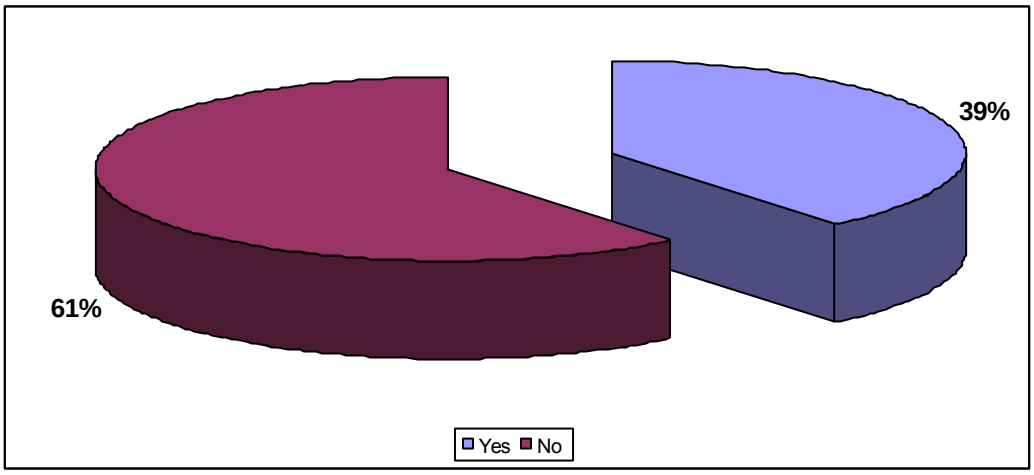
Figure 4_31 : Learners S14.8: Have you ever opened a picture sent from somebody you do not know



Lastly, it is staggering to note that Figure 4_32 shows that 39% of respondent learners have met in person with a contact they have made online. Online contacts could reveal false identities, and this behaviour by the respondent learners is very dangerous. They are placing themselves at risk due to possible curiosity and intrigue in meeting new people online, and then meeting them in person, thereby trusting

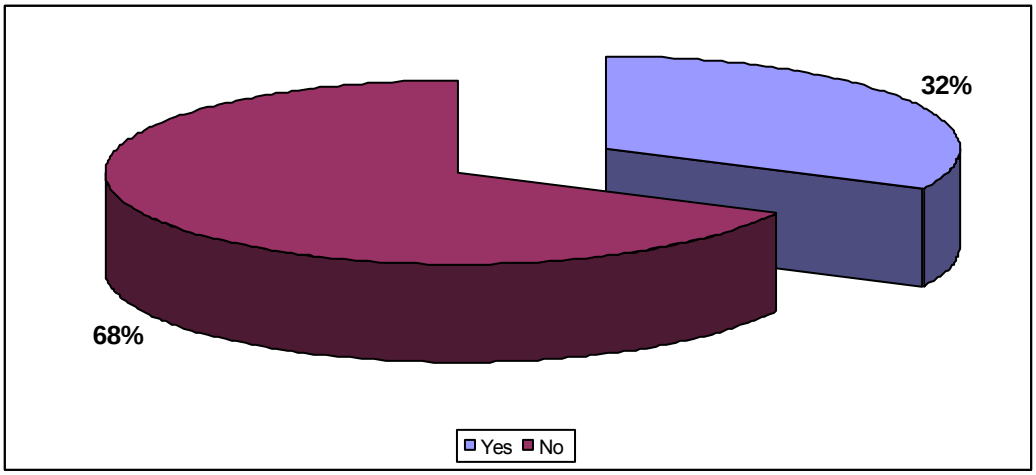
online identities. This behaviour is clearly discouraged and users are warned against doing this. However, this has not stopped 39% of users who have chosen to meet their online contacts in person.

Figure 4_32 : Learners S14.9: Have you ever met anyone in person that you have met online



32% of learners, as shown in Figure 4_33, have also considered meeting persons that they have met online. Warnings and media reports against this type of behaviour have therefore had little effect in stressing the importance of more responsible online behaviour.

Figure 4_33 : Learners S14.10: Have you ever considered meeting anyone in person that you have met online, and then changed your mind?



In summary on research question 3, it has been found that even though 91,9% of learners are aware of the dangers that can be associated with MXiT, more than half of the learners interviewed may still talk to strangers. There are also a fair proportion of learners that expose themselves to danger by talking to strangers and meeting new people online, and in so doing disregard the warning messages.

4.6 Conclusions

A total of 856 respondent learners filled in the questionnaires from the Umlazi, Pinetown and ILembe districts of KwaZulu-Natal, and a total of 13 schools participated.

The results show that just over a quarter of the parents are not aware of their children's online activities, specifically MXiT. It has been shown that there may be a lack of parent involvement, with parents not monitoring their children's (online) activities as they should. One of the contributing factors to this could be the low level of parental education, with 32,9% of parents having lower that a matric education.

45,3% in the age groups 12-13 years, 14-15 years, and 16-17 years had NOT informed their parents about MXiT use, where MXiT clearly requires all minors to inform their parents, showing that this form of parental control and monitoring is not effective. Furthermore, 37,4% of respondents in the age group 12-13 years have NOT informed their parents that they are registered on MXiT, as is required. 38% of the parents in this study are also not aware of age restrictions imposed when using MXiT. This indicates that the age restriction policies employed by MXiT may not be effective in regulating use and preventing abuse.

There could be several reasons for why children do not ask their parents for permission to use online social networking sites like MXiT. One of these reasons could be that there is a lack of communication between parents and children. Children may also be afraid to inform their parents, as their parents might make assumptions of the dangers of MXiT based on media reports, with their parents not fully understanding the benefits of MXiT. It may therefore be easier not to discuss

these issues with parents, with children preferring to keep their parents ignorant of certain issues. This lack of communication may therefore result in parents not being asked for permission to use MXiT.

Only a small proportion of MXiT chat room users are aware of warning messages related to keeping personal information private.
More than half the respondent users (54%) are not aware of the .rat command to report abuse, making this feature ineffective.

It has also been found that African users of MXiT among the sample group are less aware that non-African users of the possible dangers in using MXiT, are less aware that criminals can use fake IDs and pretend to be someone they are not, are less aware that people can get addicted to MXiT, and less aware of abduction caused through the use of MXiT. Due to socio-economic factors, it could be that Africans don't have access to various media such as radios, televisions or access to newspapers and are therefore unaware of the possible dangers of using MXiT.

It has also been concluded that even though 91,9% of learners are aware of the dangers that can be associated with MXiT, more than half of the learners interviewed (54,2%) may still talk to strangers. Furthermore, even though learners are aware of the dangers that can be associated with MXiT, they are still prepared to talk to strangers and meet new people online, thus exposing themselves to these dangers. There are also a fair proportion of users that communicate through sending and receiving pictures on MXiT, despite being aware that this can be dangerous. There are also indications of disregard for warning messages.

39% of users who have chosen to meet their online contacts in person, and 32% of respondents have also considered meeting persons that they have met online. It has been inferred that either warnings and media reports against this type of behaviour have had little effect in stressing the importance of more responsible online behaviour, or that users believe that these dangers are not applicable to themselves.

In conclusion, there is scope to improve the awareness of security guidelines applicable to MXiT. In general, African users are less aware of the possible dangers

in using MXiT as compared to other ethnic groups. There is also a disregard for certain warning messages, and users attitudes indicate that they continue to ignore warning messages and even meet their new online contacts in person. This behaviour can lead to increased risk and expose users to dangers.

Chapter 5 : Conclusions and Recommendations

5.1 Introduction

This chapter gives a summary of the main conclusions reached during the analyses and discussions in Chapter 4. It will also present the strengths and weaknesses of the study, and will conclude with areas for further research and recommendations.

The aim of this study was to understand the effectiveness of current security measures that help regulate the use of social networking sites accessed via mobile telephony, specifically MXIT. The scope of this research included an understanding of the awareness of, and attitudes towards, current security guidelines. The research objectives were stated as :-

- To understand what security guidelines are in place when using MXiT, and what are the levels of awareness of these by high school learners
- To understand the attitudes and behaviours towards security guidelines that govern the use of mobile social networking sites such as MXiT
- To determine whether general mobile security guidelines for MXiT are working to prevent abuse.

5.2 Literature Review

The review in Chapter 2 showed that there are over 19 million MXiT registered users, most of them aged between 12 and 25 years, and about 56% of them are male. It as also shown us that the secure use of MXiT is left to individuals, and for children this is left to them and their parents' approval and monitoring. The security features offered by MXiT are in the form of tips and guidelines. These include comprehensive online safety guidelines, discussion forum rules prohibiting pornography, stalking, harassment or other forms of abuse, rules to protect user confidentiality, full disclosure of consumer protection data, enhanced chat room security; a facility for users to report abuse or illegal use, peer rating and exclusion of repeat offenders from chat rooms, online support and user assistance, secure username and password logon,

user control over profiles and public information, and age restrictions limiting use to users older than 14.

The problems and benefits of using MXiT have also been described, and it has been found that MXiT is just a technology and its power lies in the hands of those who use it. It can be used for good or bad. Banning or forbidding the use of MXiT and other instant messaging services does not make the problem go away. Users and parents need to be aware of the possible dangers so that they can empower themselves to use and enjoy the great benefits of the service. According to Naik (2010 p.5), it is the responsibility of parents to ensure their children's safety. It is further stated that "Children should not be given cell phones without clear rules and information about risk. Their use should be managed and monitored. Parents should learn to use these technologies themselves and get their children to teach them if they don't know how." There are other views that MXiT should force mandatory registration "with some sort of check - credit card or faxed ID…Then they should allow only people over 18 to register - i.e. if your kid wants to use MXiT, then the parent should register for them", (WS23 2006 p.1).

It has been found that the majority of security guidelines and their successful use depend on education and awareness of what these security measures are. Secure use of mobile social networking sites such as MXiT are best regulated by parental awareness and monitoring of their child's online habits. This needs awareness of parents of technology, its uses and benefits, the associated dangers, as well as how to encourage and monitor usage of such networks.

5.3 Research Design and Methodology

The research comprised a total of 1300 learners from 15 high schools in 3 districts of KwaZulu-Natal, namely the districts of Umlazi, ILembe and Pinetown. Self-administered questionnaires were drawn up for the learners' parents as well as for the learners, with permission required from parents for learners to participate. The questionnaires were handed out to schools and administered by a nominated school representative. All questionnaires were in English, with a choice of answers for each

question, with no detailed explanations required. All indications are that the learners understood the questions and language was not an issue.

However it was found that the questionnaire could have been simplified and been more specific to the research questions. Furthermore, the research questions could also have been more specific and were quite broad. A combination of more defined research questions and a better aligned questionnaire would have led to more concrete findings. Nonetheless, the research has provided valuable insights, which are detailed in Chapter 4 and summarised below.

5.4 Summary of Findings for the Research Questions

5.4.1 Research Question 1

The research has found that the security guidelines in place when using MXiT are self-governed and in the form of guidelines and warnings. There are no security measures that are fool-proof and completely secure. The 3 main security features explored in this study are: Age Restriction, Privacy, and Reporting Abusive Users.

The Age Restriction policy states: "You must be at least 14 years old to enter into an agreement with MXiT. If you are 17 years and younger but older than 14 you will inform your parents/guardians that you have registered for, and are using the services of MXiT". Out of the total number of learners that are under the age of 18 (17 years and younger), only 54,7% have informed their parents. Possible reasons for this are a lack of communication between parents and their children, and children uncomfortable to inform their parents because of the negative publicity in the media around MXiT. 38% of parents are also not aware of age restrictions applicable when using MXiT, and therefore are not aware of the parental control and monitoring required. There may also be lack of parental involvement, with parents not monitoring their children's (online) activities as they should. The low level of parental education, with 32,9% of parents having lower that a matric education, could be a contributing factor.

A total of 89,5% of under 14s are using MXiT – these users are under-age and should not be using MXiT. Unfortunately the research was not conclusive in establishing how many of these under-age users are aware of the age restriction applicable to use MXiT. It has therefore been concluded that either the users are not aware of the age restrictions, or are possibly aware and choose to ignore it.

Users are warned about the importance of maintaining privacy when using MXiT, and are warned to keep their personal profiles confidential. The study has shown that despite these warnings, 32% of learners had revealed personal information on MXiT. Almost a third of learners (31%) use chat rooms on MXiT; however a total of 26% of learners claim that they are not aware of warnings to keep their personal information private. With such a low proportion of users aware of personal warnings when using chat rooms, it is either that these warning messages are not effective, or that users do not take heed of these warning messages or even choose to read them.

There is also a .rat command to "rat" on abusive users and report abusive language and behaviour. 46% of users are not aware of their feature, which makes its intended use very ineffective.

It may be concluded from the research that users are not fully aware of the security features when using MXiT. It is recommended that these features are made more explicit, and MXiT find a way to control and limit usage to users that are 14 years and older, perhaps by using a form of identification such as ID numbers for South African citizens.

5.4.2 Research Question 2

It can be summarised that 87% of the users in this research are aware of the possible dangers in using MXiT. These results also differ between ethnic groups. However, because of the relatively smaller number of White, Coloured and Indian users when compared to African learners in this study, comparisons were drawn between African and non-African users. The results show that :-

- 74,8% Africans are aware of the possible dangers in using MXiT, as compared to 95,0% non-Africans,
- 79,6% Africans are aware that criminals can use fake IDs and pretend to be someone they are not, as compared with 94,6% non-Africans,
- 84,1% Africans are aware that people can get addicted to MXiT, as compared with 96,6% non-Africans,
- 57,4% Africans are aware of examples where people have got abducted because of the contacts they have met using MXiT, as compared with 87,8% non-Africans.

It has therefore been concluded that African respondents as compared with non-African respondents are less aware of the possible dangers in using MXiT, less aware that criminals can use fake IDs and pretend to be someone they are not, less aware that people can get addicted to MXiT, and less aware of examples where people have got abducted because of contacts they have met using MXiT.

Based on these findings, there is scope to improve the levels of awareness of MXiT and security guidelines to users, and especially to the African population. This education can be in the form of mandatory parental consent, increased online education in the form of tips and hints, random check to test user awareness, and possibly more intervention by schools to educate children about MXiT and social networking in general.

5.4.3 Research Question 3

It has been found that even though 91,9% of learners are aware of the dangers that can be associated with MXiT, more than half of the learners interviewed (54,2%) may still talk to strangers. Furthermore, even though learners are aware of the dangers that can be associated with MXiT, they are prepared to talk to strangers and meet new people online, thus exposing themselves to these dangers. There are also a fair proportion of users that communicate through sending and receiving pictures on MXiT, despite being aware that this can be dangerous. There are also indications of disregard for warning messages.

A high proportion of 39% of users have chosen to meet their online contacts in person, and 32% of respondents have also considered meeting persons that they have met online. This is clearly very dangerous as a way to meet new people, especially given the media reports of abduction and missing children attributed to MXiT. It has been inferred that either warnings and media reports against this type of behaviour have had little effect in stressing the importance of more responsible online behaviour, or that users believe that these dangers are not applicable to themselves.

It is recommended that these dangers be made more explicit. An analogy is the tobacco industry where warnings and dangers associated with tobacco use are explicit. MXiT needs to make warnings more explicit, and test whether these warning messages are effective and sufficient.

5.5 Proposed Further Research

Even though there was a good sample selected, the researcher believes that the survey could have been improved by using a more focussed questionnaire linking more directly to the research questions. There were too many broad questions about MXiT usage in general, and this could have been more explicit linking to the 3 research questions. It is evident from this point there is a need for a more focussed questionnaire for detailed and valuable research findings.

It is also proposed that further research be conducted to understand specific habits and usage patterns based on interviews of users as well as questionnaire based research. This will provide more insights on why certain users might ignore certain warnings, and whether in fact they understand the meaning of these warnings and their possible impact.

It is also proposed to understand the differences between ethnic groups better, and why these differences exist. This may be done by focusing on African users specifically, or by choosing an equal sample between all ethnic groups.

5.6 Conclusions

This chapter concludes the research related to An Investigation of High School Learners using MXiT, and their Attitudes towards Mobile Security. The three research questions related to this topic have been answered. The research has found that the security guidelines in place when using MXiT is self-governed and in the form of guidelines and warnings, and these are not completely fool-proof. Even though there is an age restriction in place, 89,5% of under age users that participated in this research are using MXiT. Users are also not fully aware of the security features when using MXiT.

It has also been discussed that African respondents as compared with non-African respondents are less aware of the possible dangers in using MXiT, less aware that criminals can use fake IDs and pretend to be someone they are not, less aware that people can get addicted to MXiT, and less aware of examples where people have got abducted because of contacts they have met using MXiT.

Learners are aware of the dangers that can be associated with MXiT; however they are prepared to talk to strangers and meet new people online, thus exposing themselves to these dangers. There are also a fair proportion of users that communicate through sending and receiving pictures on MXiT, despite being aware that this can be dangerous. There are also indications of disregard for warning messages.

In conclusion, there is scope to improve the security measures for MXiT users, and improve the levels of education around the need to using these security features, and the possible dangers that can exist for these users.

References

Aceituno, V. (2005). "On Information Security Paradigms."

Adams, D. (2011). "History of Social Media." from http://www.instantshift.com/2011/10/20/the-history-of-social-media/.

Anderson, A. (2011). "Facebook.com hits 1 Trillion Pageviews." from http://www.keynoodle.com/facebook-com-surpasses-1-trillion-pageviews/.

Arnall, T. (2004). Mobile social software applications. from http://www.elasticspace.com/2004/06/mobile-social-software

Barker, J. (2011). "Smartphones and Tablets : More than half of all computers aren't computers anymore."

Beger, G. (2011). From „What's your ASLR' to 'Do You Wanna Go Private?'. from http://www.unicef.org/southafrica/SAF_resources_mxitstudy.pdf

Bonneau, J. (2009). "Privacy Suites : Shared Privacy for Social Networks." from http://www.cups.cs.cmu.edu/soups/2009/posters/p13-bonneau.pdf.

Borders, B. (2009). A Brief History of Social Media. from http://www.copybrighter.com/history-of-social-media

Bosch, T. (2008). "Adolescent girls' use of MXiT in Cape Town." Commonwealth Journal of Youth Studies.

Boyd, D. M. (2007). "Social network sites: Definition, history, and scholarship." Journal of Computer-Mediated Communication, 13(1), article 11.

Bremmen, N. (2010). "Why MXit is Africa's largest social network." from http://www.memeburn.com/2010/10/why-mxit-is-south-africas-largest-social-network/

Carfi, C. (2007). Social Networking for Businesses & Associations. from http://www.slideshare.net/christophercarfi/executive-briefing-social-networking-for-businesses-and-associations

Catano, N. (2009). "Poporo : A Formal Framework for Social Networking."

Chapman, C. (2011). "History and Evolution of Social Media." from http://www.ponderingtechnology.wordpress.com/2011/10/04/good-article-the-history-and-evolution-of-social-media/.

Chapman, K. (2010). "Cyberpsychology, Bevaviour, and Social Networking."

Chigona, C. (2008). "Mxit Up In The Media : Media Discourse Analysis on a Mobile Instant Messaging System."

Chigona, W. (2009). "MXiT : Uses, Perceptions and Self-Justifications." Journal of Information, Information Technology, and Organisations.

Collier, A. (2011). A Parent's Guide to Facebook. from
http://www.connectsafely.org/pdfs/fbparents.pdf

Cox, L. (2007). "Smokescreen : Flexible Privacy Controls for Presence-Sharing." from
http://www.cs.duke.edu/~varun/pubs/smokescreen.pdf

Deutsch, W. (2011). "Introduction to Electronic Access Control." from
http://www.bizsecurity.about.com/od/physicalsecurity/a/Intro_EAC.htm.

Dong, W. (2010). "Secure Friend Discovery in Mobile Social Networks." from
http://www.cs.utexas.edu/~lili/papers/pub/infocom2011.pdf

Facebook (2010). "Facebook." from
http://www.facebook.com/press/info.php?statistics.

Flora, T. (2009). "Design and Development of a Mobile Peer-to-Peer Social Networking Application." from
http://www.mendeley.com/research/design-and-development-of-a-mobile-peertopeer-social-networking-application

Francke, E. (2007). "South African Youth and Mobile Technology Impact : The MXiT Phenomenon." Proceedings of the 9th Annual Conference on World Wide Web Applications.

Freeman, J. M. (2006). MXiT : Content and Use Policy, Guidelines and Position Statement. from
http://www.mxit.com/store/portal/en/pdfs/Newmxit_lifestyle_content_and_use_policy_7_sept_2006.pdf

Gross, R. (2005). "Information Revelation and Privacy in Online Social Networks." from
http://www.dl.acm.org/citation.cfm?id=1102214

Harriman, G. (2010). E-Learning Resources. from
http://www.itdl.org/Journal/Oct_10/article02.htm

Hazlett, B. (2008). "Social Networking Statistics & Trends." from
http://www.slideshare.net/onehalfamazing/social-networking-statistics-and-trends-presentation

Heunis, H. (2009). Innovation and ICT in Africa. from
http://www.africaneconomicoutlook.org/

Hiltz, S. R. (1993). The Network Nation : Human Communication via Computer, MIT Press Cambridge, MA, USA

Hollands, B. (2007). Sordid Sex Scare on Cell Phone Chat System. Weekend Post. from
http://www.link.wits.ac.za/journal/J09-Chigona.pdf

Jacobs, A. (2010). "MXit bullies threaten School children." from
http://www.news24.com/SouthAfrica/News/MXit-bullies-threaten-school-children-20101017.

Jansen, W. (2010). "Towards a Unified Framework for Mobile Device Security." from
http://www.csrc.nist.gov/mobileSecurity/publications.html

Johnson, B. (2010). ""MXiT : Angel or Demon."." from
http://www.cellfhelp.co.za.

Keating, C. (2006). "Schools Seek to Ban Addictive MXiT." from
http://www.iol.co.za/news/south-africa/schools-seek-to-ban-addictive-mxit-1.290620.

Keller, G. (2000). "Statistics for Management and Economics."

Knight, J. (2011). Social Media Overview. from
http://www.ucsf.edu/about/social-media-overview

Lappas, T. (2010). Social Networking : Finding Effectors in Social Networks. from
http://www.kddlab.di.uoa.gr/research.php

Leelachand, P. (2011). "Social Networking Sites - The 21st Century Craze." from
http://www.defimedia.info/articles/11829/1/Social-networking-sites--The-21st-century-craze/Page1.html.

Leem, K. (2005). "Security Threats and their Countermeasures of Mobile Portable Computing Devices in Ubiquitous Computing Environments.".

Lenhart, A. (2007). Teens, Privacy and Online Social Networks. How Teens Manage their Online Identities and Personal Information in the age of MySpace.

Li, K. A. (2008). People Tones : A System for the Detection and Notification of Buddy Proximity on Mobile Phones.

Lombard, A. (2011) Cops Track MXit Porn Ring. from
http://www.news24.com/SouthAfrica/News/Cops-track-MXit-porn-ring-20110820-2

Manners, T. (2009). "MXit survey highlights abuse." from
http://www.mybroadband.co.za/news/cellular/10778-mxit-survey-highlights-abuse.html.

McDowell, M. (2009). Staying Safe on Social Network Sites. from http://www.us-cert.gov/cas/tips/ST06-003.html

McLaren, J. (2009). ""Why Teens Love MXiT?"." from http://www.parent24.com/Teen13-18/developmentbehaviour/why-teens-love-mxit

Merz, B. (2010). "MXiT." from http://www.sacareer.co.za.

Mjelly, R. (2009). MXit-South Africa's No 1 Mobile Social Networking Startup. from http://www.mobileindustryreview.com/2009/02/mxit.htm

Mooney, T. (2011). ""Where are the online predators hanging out"." from http://www.blogs.mcafee.com/author/tracy-mooney.

Muller, R. (2009). "MXit lashes out at poor media reporting." from http://www.mybroadband.co.za/news/cellular/9118-mxit-lashes-out-at-poor-media-reporting.html.

Muller, R. (2009) MXit registrations surpass 14 million. from http://www.mybroadband.co.za/news/cellular/8785-mxit-registrations-surpass-14-million.html

Muller, R. (2010) South African cellphone facts revealed. from http://www.mybroadband.co.za/news/cellular/13080-South-African-cellphone-facts-revealed.html

Myeni, S. (2010). MXiT. from http://www.fpb.gov.za/index.php?option=com_content&view=article&id=171&Itemid=183

NA1 (2010). Teens Drawn to 'Toilet' Tech Site. Sunday Tribune, *7 November 2010.*

NA2 (2009). New Teen Porn Shocker on MXiT. The Citizen, *25 February 2009*.

NA3 (2008). MXiT an Easy Route to Crime. Beeld, *1 August 2008*.

NA4 (2006). Schools Seek to Ban "Addictive" MXiT. Cape Argus, *23 August 2006*.

Naik, S. (2010). ""Who is your child talking to on MXiT?"." from http://www.girlsnet.org.za/news/whoyourchildistalkingtoonmxit.

Nickson, C. (2009). The History of Social Networking. Digital Trends. from http://www.digitaltrends.com/features/the-history-of-social-networking/

Nielson (2009). Global Faces and Networked Places. A Nielson Report on Social Networking's New Global Footprint.

Nunnally, J. C. (1978). Psychometric Theory.

Oppeng, T. (2011). "MXit, Africa's Biggest Mobile Social Network has been Acquired." from
http://www.alltopstartups.com.

Parker, M. (2010). "The Growth of Mobile Phones." from
http://www.cellfhelp.co.za.

Perelson, S. (2006). "An Investigation into Access Control for Mobile Devices."

Perey, C. (2010). Mobile Social Networking. from
http://www.slideshare.net/CHmomo/mobile-social-networking-trends-and-forecasts-from-the-informa-2009-market-research-report

Reuters, R. (2011). "Social Networking boosts teen drug abuse." from
http://www.news.mobile.msn.com.

Reynaldo, J. (1999). "Cronbach's Alpha : A Tool for Assessing the Reliability of Scales". from
http://www.joe.org/joe/1999april/tt3.php

Riabinin, Y. (2008). Internet Relay Chat : Stopping the Loss on Information. from
http://www.mindigo.com/Report_Final_PDF.pdf

Rosen, C. (2007). "Virtual Friendship and the New Narcissism." from
http://www.faculty.wiu.edu/CB-Dilger/f09/101/rosen-narcisissm.pdf

Rosenbush, S. (2005) News Corp.'s Place in MySpace. Bloomberg Businessweek

Schmidt, E. (2011). "Mobile as a Trillion Dollar Industry." from
http://www.consultantvalueadded.com/2011/03/07/mobile-as-a-trillion-dollar-industry-check-this/

Schoneburg, E. (2011) Artificial Life partners with MXiT. from
http://www.artificial- life.com/en/investor_relations/press_releases
/2011/news/press_20110722en

Schroeder, S. (2010). "Social Networks are Becoming a Security Risk." from
http://www.mashable.com/2010/02/01/social-networks-security-risk/

Shallcross, K. (2010). "Some Alarming Stats Concerning Online Activity."

Shannon, V. (2008) Social Networking Moves to the Cellphone New York Times

Smillie, S. (2010). Teen in MXit Rape Ordeal. IOL News. from
http://www.iol.co.za/news/south-africa/teen-in-mxit-rape-ordeal-1.672193

Solms, R. V. (2011). "Children at risk of online bullying." from
http://www.mg.co.za/article/2011-02-04-children-at-risk-of-online-bullying.

Sorhum, K. K. (2010). The Business Impacts of Social Media and Social Networking.

Stelzner, M. A. (2011). Social Media goes Mainstream in South Africa.

Streicher, P. (2011). "SMS, the most expensive yet also most used data application." from
http://www.bulksms.2way.co.za/c/BulkSMS-SMS-the-most-expensive-yet-also-the-most-used-data-application.pdf.

Sway, A. (2011). "Is Social Media Anti-Social." from
http://www.rinf.com/alt-news/social-media-2/is-social-media-anti-social/10251/.

Terry, L. (2011). Taming the Wild West of Executives' Mobile Devices.

Thomas, R. (2007). MXiT Parents Guide. from
http://www.ramonthomas.com/download/mxit/

Thomas, R. (2010) Mxit declares war on porn. from
http://www.mybroadband.co.za/news/cellular/11904.html

Thomas, R. (2011). "Parents Guide to MXit." from
http://www.docstoc.com/docs/74898087/Parents-Guide-to-MXit.

Thornton, L. (2007). Protecting Minors from Harmful Content via Mobile Phones.

Toit, J. D. (2011). MXiT reinvents itself. from
http://www.themediaonline.co.za/20011/07

Trennery, S. (2010). "Herman Heunis." from
http://www.izimvo.com/herman-heunis/.

Valdecantos, C. (2011). Two Billion Internet users Worldwide and Mobile Phone Users Increases. MercoPress. from
http://www.en.mercopress.com/2011/01/27/two-billion-internet-users-worldwide-and-mobile-phone-users-increases

Vecchiatto, P. (2009) Mxit to flex its muscle. ITWeb from
http://www.itweb.co.za/index.php?option=com_content&view=article&id=14187:m xit-to-flex-its-muscle&catid=76:cellular

Waldvogel, S. K. (2008). Consistent Deniable Lying : Privacy in Mobile Social Networks. from
http://www.pervasive2008.org/Papers/Workshop/w1-03.pdf

Wauters, R. (2011). "Social Network Pioneer Friendster to erase all user photos and blogs." from
http://www.techcrunch.com.

Westfall, L. (2009). Sampling Methods. The Certified Software Quality Engineer Handbook.

Weyhrich, S. (2011). "The Story of the "Most Personal Computer"!". from http://www.apple2history.org/history/ah22/.

Whitworth, C. (2011). "The Death of MySpace." from http://www.youngacademic.co.uk/features/the-death-of-myspace-young-academic-columns-953.

Willard, N. (2007). Schools and Online Social Networking. from http://www.csriu.org/cyberbully/docs/cbcteducator.pdf

Wilson, L. (2011). "MXiT Up" to reach South Africans. from http://www.2011globalmarketing.wordpress.com/2011/07/24/mxit-up-to-reach-south-africans/

WS1 (2009). "MXiT and Your Business." from http://www.mxit.com/web/business.htm.

WS2 (2009). ""MXiT Moola is now available on cellphone banking from FNB"." from https://www.fnb.co.za/frames/content/campaign/mixit/index.html.

WS3 (2008). "Dr Math Rocks:! Using Instant Messaging to Help Pupils with their Mathematics Homework." from http://www.researchspace.csir.co.za

WS4 (2010). "MXiT." from http://www.ambientmedia.co.za/mxit.htm.

WS5 (2006). "MXiT - All You Need to Know." Joy. from http://www.joymag.co.za/article.php.

WS6 (2009). "MXit urges use of common sense after teen's rape." from http://www.highbeam.com/doc/1G1-214793942.html.

WS7 (2010). "The Cellphone: A South African's Best Friend." from http://www.dialdirect.co.za/The-Cellphone-South-Africans-Best-Friend.

WS8 (2010). "Mobile Stats - Mobile Consumption in S.A." Yonder Mobile Media. from http://www.yonder.co.za/home/static/en_US/id/131/title/mobile+stats.html.

WS9 (2009). "MXiT - South Africa's No1 Mobile Social Networking Startup." from http://www.mobileindustryreview.com/2009/02/mxit.html.

WS10 (2011). "MXiT." from http://www.mxit.com/.

WS11 (2011). Repositioning for the Future. from http://www.capetown.gov.za/en/DesignCapital/Documents/BIDBOOK_CS_3_2_Queation_43.pdf

WS12 (2011). "MXiT Safety and Forum Guide." from http://www.mxit.co.za/.

WS13 (2009). "Mxit Legal Content Policy." from http://www.mxit.com/content/ap/en/legal_content_policy.

WS14 (2010). "The Threat to Anonymous Online Speech ". from http://www.cyberslapp.org/faq.cfm.

WS15 (2009). "Unethical Lawyer - FBI, BAR, and Local Authorities Contacted." from http://www.nobarack08.wordpress.com/2009/12/03/unethical-lawyer-breaks-law.

WS16 (2011). "Why is MXit Dangerous." from http://www.knowswhy.com/why-is-mxit-dangerous/.

WS17 (2011). "Online Predators." from http://www.familysafecomputers.org/predators.htm.

WS18 (2010). "Social Networking Services and Privacy Issues." from https://www.cippguide.org/2010/09/28/social-networking-services-privacy-issues/.

WS19 (2011). "Date Security Policy." from http://www.tradecard.com/privacy/data.html.

WS20 (2011). "Biometrics in Cell Phones." from http://www.thirdfactor.com/2011/06/22/experts-make-case-for-biometrics-in-cell-phones.

WS21 (2010). "The Secret Online Lives of Teens." from http://www.us.mcafee.com/en-us/local/docs/lives_of_teens.pdf

WS22 (2010). "European Network and Information Security Agency." from http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens.

WS23 (2006). ""A parent's suggestion to MXiT developers."." from http://www.mybroadband.co.za/vb/showthread.php/57107aparentssuggestiontomxitdevelopers.

WS24 (2011). "Sophos Security Threat Report reveals increase in social networking security threats." from http://www.sophos.com/en-us/press-office/press-releases/2011/01/threat-report-2011.aspx.

Ying, L. (2008). "Users Perception of Mobile Information Security." from
http://www.cs.cmu.edu/~haiyiz/Abstract.pdf

Zhu, Y. (2010). A Collaborative Framework for Privacy Protection in Online Social Networks. from
http://www.eprint.iacr.org/2010/491.pdf

Appendix A : Parent's Research Questionnaire

Place a tick ✓ in the in the box to select your answer.
Please only select 1 answer for every question.
Please fill in ALL questions.

Part 1 : Personal Particulars

1. Highest qualification
- ☐ Tertiary education
- ☐ Matric (Grade 12)
- ☐ Other

2. Ethnic Group
- ☐ African
- ☐ Coloured
- ☐ Asian
- ☐ White
- ☐ Other

	YES	NO
3.1 Do you own a mobile cellular phone?		
3.2 Have you heard of what MXiT is?		
3.3 Are you aware of whether your child / children are using MXiT?		
3.4 Has your child ever asked for permission to use MXiT?		
3.5 Are you aware of the requirements that are in place for children to use MXiT, such as :-		
3.5.1 Age restrictions		
3.5.2 Parents being able to block chatrooms on MXiT		
3.5.3 Being able to report abuse while using MXiT		
3.6 Have you heard of some of the dangers associated with using MXiT inappropriately, such as :-		
3.6.1 Addiction, and children getting addicted to MXiT		
3.6.2 Criminals using fake IDs		
3.6.3 Communicating with strangers on MXiT		
3.6.4 Abduction of children that have been using MXiT		

Thank you for your time in filling in this questionnaire.

Appendix B : Learner's Research Questionnaire

Place a tick ✓ in the box to select your answer.
Please only select 1 answer for every question.
Please fill in ALL questions.

Part 1 : Personal Particulars

1. Age : _____years

2. Gender : □ Male □ Female

3. Grade
□ Grade 8 □ Grade 9 □ Grade 10 □ Grade 11

4. Ethnic Group
□ African □ Coloured □ Asian □ White
□ Other

Part 2 : General Questions to understand use of MXiT

Section 1

	YES	NO
5.1 I have my own mobile cellular phone		
5.2 I have heard about and use MXiT		

6. I have been using MXiT

□ For years
□ For about the last year
□ For less than 6 months
□ For the last month only

7. I use MXiT mainly from

□ My own mobile phone
□ A friend's mobile phone
□ My parents mobile phone
□ Other

8. I use MXiT

□ Every day
□ At least 3 times a week

- At least once per week
- Less than once per week

9. I normally use MXiT

- Anytime day or night
- Only on weekends
- Only during school hours
- Anytime but not during school hours

10. I am most likely to use MXiT

- Only when I am alone
- When I am around friends
- When I am around friends or family
- Not when I am around family

11. When I use MXiT, it is normally

- To send important messages only
- To socialise and chat to my friends
- To communicate with my family
- Because I am bored

12. When I use MXiT, it is normally

- Less than 5 minutes
- Less than 15 minutes
- Less than 30 minutes
- At least for an hour

13. I use MXiT

- For using the cheap message service
- Only for the chatrooms
- To send and receive music and / or pictures
- All of the above

Section 2

	YES	NO
14.1 I use MXiT chat rooms		
14.2 Are you aware of the rules that exist in using MXIT chat rooms?		
14.3 When entering chat rooms, are you warned about keeping your personal information private?		
14.4 Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details?		
14.5 Have you shared your cell phone password with friends or anyone else?		
14.6 Have you shared your MXIT pin with friends or anyone else?		
14.7 Using MXiT, have you communicated with people you have not met and do not know?		
14.8 Have you ever opened a picture sent from somebody you do not know?		
14.9 Have you ever met anyone in person that you have met online?		
14.10 Have you ever considered meeting anyone in person that you have met online, and then changed your mind?		
14.11Have you informed your parents that you have registered on MXIT?		
14.12 Are you aware that chat rooms have moderators that monitor the conversation?		
14.13 Are you aware of the .rat command to report abuse on MXIT?		
14.14 Are you aware that you can set up your own chatroom, and can limit this only to people you know?		

Section 3

	ALWAYS	SOME-TIMES	NEVER
15.1 The use of MXIT can be dangerous and open to abuse			
15.2 My cell phone password is kept secret at all times			
15.3 My MXIT password is important to keep confidential			
15.4 MXIT is fun and is not dangerous at all			
15.5 I only use MXIT to talk to people I know			
15.6 I talk to strangers on MXIT			
15.7 I download files from people I do not know			
15.8 I send pictures to people I do not know			
15.9 I have online friendships or relationships with people I have not met			
15.10 I use MXiT to meet new people			
15.11 I don't mind who I talk to in chat rooms			
15.12 I use MXIT to only chat to people I know			
15.13 If there is abuse on MXIT, I inform my parents			

Section 4

		YES	NO
16.1 Are you aware of the possible dangers in using MXiT			
16.2 Are you aware that criminals can use fake IDs and pretend to be someone they are not			
16.3 Do you know that people can get addicted to MXiT			
16.4 Have you heard of examples where people have got abducted because of the contacts they have met using MXiT			

Thank you for your time in filling in this questionnaire.

Appendix C : Parental Consent

UNIVERSITY OF KWAZULU-NATAL
School of Information Systems & Technology

PARENTAL CONSENT TO PARTICIPATE IN RESEARCH

M Com Research Project
Researcher: Mrs N Bhoola (031 - 5630266)
Supervisor: Professor M. Maharaj (031 260 8023)
Research Office: Ms P Ximba 031-2603587

Consent

I have read the above information about *the use of Mxit among High School Learners and their Attitudes towards Mobile Security Framework* and have been given an opportunity to ask questions. By signing this I agree to allow my child to participate in this study and I have been given a copy of this signed consent document for my own records. I understand that I can change my mind and withdraw my consent at any time.

By signing this consent form I understand that I am not giving up any legal rights.

_____ _____

Parent or Legal Guardian Signature Date

Name of Child _____

Appendix D : Sample of Letter Requesting Permission to do Research

Name of School
Address 1
Address 2
Code

21 January 2010

TO WHOM IT MAY CONCERN

We have been approached by Mrs Nisha Bhoola to conduct research for a Masters Project entitled : “An Investigation of High School Learners using MXit, and their Attitudes towards Mobile Security Frameworks”.

I understand that the research will be in the form of questionnaires handed out to pupils, as well as to their parents seeking their permission. The research will be conducted with pupils from grades 8 to 11 inclusive. The research will be completed in the first term of 2010.

I hereby grant Mrs Nisha Bhoola permission to conduct research in the form of questionnaire surveys to pupils from grades 8 to 11 in my school.

Yours faithfully,

Name of Principal

Appendix E : Analyses of Variance (ANOVA)

If p value is less than or equal $p \leq 0.05$, statistically there is significance difference between groups' opinions. If p value is greater than $p > 0.05$, statistically there is NO significance difference between groups opinions.

Note: p indicates probability

District Groups

		Sum of Squares	df	Mean Square	Sig.
S15.1	Between Groups	0.266	2	0.133	0.61
	Within Groups	222.954	829	0.269	
	Total	223.22	831		
S15.2	Between Groups	5.307	2	2.653	0
	Within Groups	274.759	829	0.331	
	Total	280.066	831		
S15.3	Between Groups	8.412	2	4.206	0
	Within Groups	257.086	829	0.31	
	Total	265.499	831		
S15.4	Between Groups	1.265	2	0.633	0.149
	Within Groups	274.716	829	0.331	
	Total	275.981	831		
S15.5	Between Groups	17.445	2	8.722	0
	Within Groups	401.207	828	0.485	
	Total	418.652	830		
S15.6	Between Groups	8.469	2	4.235	0
	Within Groups	378.01	829	0.456	
	Total	386.48	831		
S15.7	Between Groups	0.62	2	0.31	0.456
	Within Groups	326.798	829	0.394	
	Total	327.418	831		
S15.8	Between Groups	1.598	2	0.799	0.061
	Within Groups	235.631	829	0.284	
	Total	237.23	831		
S15.9	Between Groups	6.74	2	3.37	0.001
	Within Groups	378.448	829	0.457	
	Total	385.188	831		
S15.10	Between Groups	5.584	2	2.792	0.007
	Within Groups	463.473	829	0.559	
	Total	469.058	831		
S15.11	Between Groups	0.285	2	0.142	0.769
	Within Groups	448.772	828	0.542	
	Total	449.057	830		
S15.12	Between Groups	20.649	2	10.324	0
	Within Groups	426.308	829	0.514	
	Total	446.957	831		
S15.13	Between Groups	15.192	2	7.596	0
	Within Groups	617.864	828	0.746	
	Total	633.057	830		

The ANOVA test results reveal there is no statistically significance difference in perceptions of different district groups respondents towards the research statements S15.1, S15.4, 15.7, 15.8 and 15.11, because these statements p significance values are 0.610, 0.149, 0.456, 0.061 and 0.769 and these values are above 0.05 (This means different district groups respondents have almost similar perceptions towards these statements and there is no huge difference in different groups respondent's opinions towards these study statements).

The ANOVA test results reveal there is statistically significance difference in perceptions of different district groups respondents towards the research statements S15.2, S15.3, S15.5, 15.6, 15.9, 15.10, 15.12 and 15.13 because these statements p significance values are 0.000, 0.000, 0.000, 0.000, 0.001, 0.007, 0.000 and 0.000 and these values are below 0.05 (This means different district groups respondents have significant different perceptions towards these statements and there is adequate difference in different groups respondent's opinions towards these study statements).

Age

		Sum of Squares	df	Mean Square	Sig.
S15.1	Between Groups	2.013	3	0.671	0.057
	Within Groups	221.207	828	0.267	
	Total	223.22	831		
S15.2	Between Groups	2.765	3	0.922	0.042
	Within Groups	277.301	828	0.335	
	Total	280.066	831		
S15.3	Between Groups	1.372	3	0.457	0.232
	Within Groups	264.127	828	0.319	
	Total	265.499	831		
S15.4	Between Groups	1.962	3	0.654	0.116
	Within Groups	274.019	828	0.331	
	Total	275.981	831		
S15.5	Between Groups	13.997	3	4.666	0
	Within Groups	404.655	827	0.489	
	Total	418.652	830		
S15.6	Between Groups	31.986	3	10.662	0
	Within Groups	354.494	828	0.428	
	Total	386.48	831		
S15.7	Between Groups	11.583	3	3.861	0
	Within Groups	315.835	828	0.381	
	Total	327.418	831		
S15.8	Between Groups	3.797	3	1.266	0.004
	Within Groups	233.433	828	0.282	
	Total	237.23	831		
S15.9	Between Groups	20.421	3	6.807	0
	Within Groups	364.766	828	0.441	
	Total	385.188	831		
S15.10	Between Groups	21.95	3	7.317	0
	Within Groups	447.107	828	0.54	
	Total	469.058	831		
S15.11	Between Groups	13.984	3	4.661	0
	Within Groups	435.073	827	0.526	
	Total	449.057	830		
S15.12	Between Groups	22.18	3	7.393	0
	Within Groups	424.777	828	0.513	
	Total	446.957	831		
S15.13	Between Groups	57.584	3	19.195	0
	Within Groups	575.472	827	0.696	
	Total	633.057	830		

The ANOVA test results reveal there is no statistically significance difference in perceptions of different age groups respondents towards the research statements S15.1, S15.3, and 15.4 because these statements p significance values are 0.057, 0.232, 0.116 and these values are above 0.05 (This means different age groups respondents have almost similar perceptions towards these statements and there is no huge difference in different groups respondent's opinions towards these study statements).

The ANOVA test results reveal there is statistically significance difference in perceptions of different age groups respondents towards the research statements S15.2, S15.5, 15.6, 15.7, 15.8, 15.9, 15.10, 15.11, 15.12 and 15.13 because these statements p significance values are 0.042, 0.000, 0.000, 0.000, 0.004, 0.000, 0.000, 0.000, 0.000 and 0.000 and these values are below 0.05 (This means different district groups respondents have significant different perceptions towards these statements and there is adequate difference in different groups respondent's opinions towards these study statements).

Grade

		Sum of Squares	df	Mean Square	Sig.
S15.1	Between Groups	0.739	3	0.246	0.432
	Within Groups	222.481	828	0.269	
	Total	223.22	831		
S15.2	Between Groups	0.089	3	0.03	0.967
	Within Groups	279.977	828	0.338	
	Total	280.066	831		
S15.3	Between Groups	0.299	3	0.1	0.817
	Within Groups	265.2	828	0.32	
	Total	265.499	831		
S15.4	Between Groups	2.796	3	0.932	0.038
	Within Groups	273.185	828	0.33	
	Total	275.981	831		
S15.5	Between Groups	4.726	3	1.575	0.024
	Within Groups	413.927	827	0.501	
	Total	418.652	830		
S15.6	Between Groups	25.846	3	8.615	0
	Within Groups	360.634	828	0.436	
	Total	386.48	831		
S15.7	Between Groups	9.689	3	3.23	0
	Within Groups	317.729	828	0.384	
	Total	327.418	831		
S15.8	Between Groups	2.231	3	0.744	0.05
	Within Groups	234.999	828	0.284	
	Total	237.23	831		
S15.9	Between Groups	9.401	3	3.134	0
	Within Groups	375.787	828	0.454	
	Total	385.187	831		
S15.10	Between Groups	14.05	3	4.683	0
	Within Groups	455.008	828	0.55	
	Total	469.058	831		
S15.11	Between Groups	10.241	3	3.414	0
	Within Groups	438.816	827	0.531	
	Total	449.057	830		
S15.12	Between Groups	12.179	3	4.06	0
	Within Groups	434.778	828	0.525	
	Total	446.957	831		
S15.13	Between Groups	51.443	3	17.148	0
	Within Groups	581.613	827	0.703	
	Total	633.057	830		

The ANOVA test results reveal there is no statistically significance difference in perceptions of different study grade respondents towards the research statements S15.1, S15.2 and 15.3 because these statements p significance values are 0.432, 0.967 and 0.817 and these values are above 0.05 (This means different study grade respondents have almost similar perceptions towards these statements and there is no huge difference in different groups respondent's opinions towards these study statements).

The ANOVA test results reveal there is statistically significance difference in perceptions of different study grade respondents towards the research statements S15.4, 15.5, 15.6, 15.7, S15.8, 15.9, S15.10, S15.11, S15.12 and 15.13 because these statements p significance values are 0.038, 0.024, 0.000, 0.000, 0.050, 0.000, 0.000, 0.000, 0.000 and 0.000 and these values are below 0.05 (This means different study grade respondents have significant different perceptions towards these statements and there is adequate difference in different groups respondent's opinions towards these study statements).

For research questions 16.1 to 16.4 inclusive, the following null hypothesis was assumed : each ethnic group has the same incidence of "yes' responses, as this would be expected in a normal distribution. The alternative hypothesis would be that the responses from the African respondents would be distinct from the responses of the non-African respondents. When using Chebychev's Theorem to test for significant differences, the following method was employed :-

- Calculate a standard deviation for the sample
- Determine by how many standard deviations away from the overall single mean the African mean is
- Based on the number of standard deviations, it helps understand how probable it is that the observation is no different to the overall population

Data showing Z values (No. of Standard Deviations from the Mean)

		Frequency	Frequency of "Yes" Responses	Probability	Z	Sigma
16.1	African	333	249	0.748		0.018
	Non-African	499	474	0.950		0.015
	Total	832	723	0.869		
	Difference			0.202	8.467	0.024
16.2	African	333	265	0.796		0.017
	Non-African	499	472	0.946		0.014
	Total	832	737	0.886		
	Difference			0.150	6.670	0.023
16.3	African	333	280	0.841		0.015
	Non-African	499	482	0.966		0.012
	Total	832	762	0.916		
	Difference			0.125	6.368	0.020
16.4	African	333	191	0.574		0.024
	Non-African	499	438	0.878		0.019
	Total	832	629	0.756		
	Difference			0.304	10.009	0.030

Given that the standard deviations (Z) above for each of questions 16.1 to 16.4 inclusive are greater than 6, the p value is 0. This shows clearly that the null hypothesis is not valid, and that the responses of the African respondents are significantly different to that of the non-African respondents for these questions.

Appendix F : Descriptive Statistics

Learners

Name of District where School is Located

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ILembe	169	19.7	19.7	19.7
	Pinetown	327	38.2	38.2	57.9
	Umlazi	360	42.1	42.1	100.0
	Total	856	100.0	100.0	

Age group of respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	12 -13 yrs	146	17.1	17.1	17.1
	14 - 15 yrs	351	41.0	41.0	58.1
	16 - 17 yrs	307	35.9	35.9	93.9
	18 - 20 yrs	52	6.1	6.1	100.0
	Total	856	100.0	100.0	

Gender of the Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	359	41.9	41.9	41.9
	Female	497	58.1	58.1	100.0
	Total	856	100.0	100.0	

Respondent Studying Grade

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Grade 8	179	20.9	20.9	20.9
	Grade 9	257	30.0	30.0	50.9
	Grade 10	218	25.5	25.5	76.4
	Grade 11	202	23.6	23.6	100.0
	Total	856	100.0	100.0	

Respondent Ethnic Group

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	African	342	40.0	40.0	40.0
	Coloured	33	3.9	3.9	43.8
	Asian	452	52.8	52.8	96.6
	White	18	2.1	2.1	98.7
	Other	11	1.3	1.3	100.0
	Total	856	100.0	100.0	

Question 5.1 : I have my own mobile cellular phone

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	675	78.9	78.9	78.9
	No	181	21.1	21.1	100.0
	Total	856	100.0	100.0	

Question 5.2 : I have heard about and use MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	789	92.2	92.2	92.2
	No	67	7.8	7.8	100.0
	Total	856	100.0	100.0	

Question 6 : I have been using MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	For years	332	38.8	42.1	42.1
	For about the last year	211	24.6	26.7	68.8
	For less than 6 Months	115	13.4	14.6	83.4
	For the Last month only	131	15.3	16.6	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
Total		856	100.0		

Question 7 : I use MXiT mainly from

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	My Own mobile phone	598	69.9	75.8	75.8
	A friend's mobile phone	79	9.2	10.0	85.8
	My parents mobile phone	73	8.5	9.3	95.1
	Other	39	4.6	4.9	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
Total		856	100.0		

Question 8 : I use MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Every day	369	43.1	46.8	46.8
	At least 3 times a week	179	20.9	22.7	69.5
	At least once per week	111	13.0	14.1	83.5
	Less than once per week	130	15.2	16.5	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
Total		856	100.0		

Question 9 : I normally use MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Anytime day or night	267	31.2	33.8	33.8
	Only on weekends	194	22.7	24.6	58.4
	Only during school hours	7	.8	.9	59.3
	Anytime but not during school hours	321	37.5	40.7	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
	Total	856	100.0		

Question 10 : I am most likely to use MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Only when I am alone	378	44.2	47.9	47.9
	When I am around friends	95	11.1	12.0	59.9
	When I am around friends or family	203	23.7	25.7	85.7
	Not when I am around family	113	13.2	14.3	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
	Total	856	100.0		

Question 11 : When I use MXiT, it is normally

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	To send important messeges only	72	8.4	9.1	9.1
	To socialise and chat to my friends	510	59.6	64.7	73.9
	To communicate with my family	32	3.7	4.1	77.9
	Because I am bored	174	20.3	22.1	100.0
	Total	788	92.1	100.0	
Missing	System	68	7.9		
	Total	856	100.0		

Question 12 : When I use MXiT it is normally

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 5 mins	69	8.1	8.7	8.7
	Less than 15 mins	110	12.9	13.9	22.7
	Less than 30 mins	164	19.2	20.8	43.5
	At least for an hour	446	52.1	56.5	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
Total		856	100.0		

Question 13 : I use MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	For using the cheap message service	452	52.8	57.3	57.3
	Only for the chatrooms	52	6.1	6.6	63.9
	To send and receive music / pics	58	6.8	7.4	71.2
	All of the above	227	26.5	28.8	100.0
	Total	789	92.2	100.0	
Missing	System	67	7.8		
Total		856	100.0		

Question 14.1 : I use MXiT chat rooms

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	259	30.3	31.0	31.0
	No	577	67.4	69.0	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.2 : Are you aware of the rules that exist in using MXiT chat rooms ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	568	66.4	67.9	67.9
	No	268	31.3	32.1	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.3 : When entering chat rooms, are you warned about keeping your personal information private ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	620	72.4	74.3	74.3
	No	215	25.1	25.7	100.0
	Total	835	97.5	100.0	
Missing	System	21	2.5		
Total		856	100.0		

Question 14.4 : Have you ever revealed personal information on MXiT previously, for eg. your real name, telephone number, home address, or any other personal details ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	268	31.3	32.1	32.1
	No	568	66.4	67.9	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.5 : Have you shared your cell phone password with friends or anyone else ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	158	18.5	18.9	18.9
	No	678	79.2	81.1	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.6 : Have you shared your MXiT pin with friends or anyone else ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	174	20.3	20.8	20.8
	No	662	77.3	79.2	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.7 : Using MXiT, have you communicated with people you have not met and do not know ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	480	56.1	57.4	57.4
	No	356	41.6	42.6	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.8 : Have you ever opened a picture sent from somebody you do not know?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	411	48.0	49.2	49.2
	No	425	49.6	50.8	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.9 : Have you ever met anyone in person that you have met online ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	327	38.2	39.1	39.1
	No	509	59.5	60.9	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.10 : Have you ever considered meeting anyone in person that you have not met online, and then changed your mind ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	269	31.4	32.2	32.2
	No	566	66.1	67.8	100.0
	Total	835	97.5	100.0	
Missing	System	21	2.5		
Total		856	100.0		

Question 14.11 : Have you informed your parents that you have registered on MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	479	56.0	57.3	57.3
	No	357	41.7	42.7	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.12 : Are you aware that chat rooms have moderators that monitor the conversation ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	381	44.5	45.6	45.6
	No	455	53.2	54.4	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.13 : Are you aware of the .rat command to report abuse on MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	449	52.5	53.7	53.7
	No	387	45.2	46.3	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 14.14 : Are you aware that you can set up your own chatroom, and can limit this only to people you know ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	589	68.8	70.5	70.5
	No	247	28.9	29.5	100.0
	Total	836	97.7	100.0	
Missing	System	20	2.3		
Total		856	100.0		

Question 15.1 : The use of MXiT can be dangerous and open to abuse

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	167	19.5	20.1	20.1
	Some times	597	69.7	71.8	91.8
	Never	68	7.9	8.2	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.2 : My cell phone password is kept secret at all times

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	631	73.7	75.8	75.8
	Some times	149	17.4	17.9	93.8
	Never	52	6.1	6.3	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.3 : My MXiT password is important to keep confidential

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	680	79.4	81.7	81.7
	Some times	97	11.3	11.7	93.4
	Never	55	6.4	6.6	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.4 : MXiT is fun and not dangerous at all

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	136	15.9	16.3	16.3
	Some times	556	65.0	66.8	83.2
	Never	140	16.4	16.8	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.5 : I only use MXiT to talk to people I know

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	380	44.4	45.7	45.7
	Some times	331	38.7	39.8	85.6
	Never	120	14.0	14.4	100.0
	Total	831	97.1	100.0	
Missing	System	25	2.9		
Total		856	100.0		

Question 15.6 : I talk to strangers on MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	94	11.0	11.3	11.3
	Some times	317	37.0	38.1	49.4
	Never	421	49.2	50.6	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.7 : I download files from people I do not know

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	63	7.4	7.6	7.6
	Some times	216	25.2	26.0	33.5
	Never	553	64.6	66.5	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.8 :I send pictures to people I do not know

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	37	4.3	4.4	4.4
	Some times	149	17.4	17.9	22.4
	Never	646	75.5	77.6	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.9 : I have online friendships or relationships with people I have not met

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	89	10.4	10.7	10.7
	Some times	264	30.8	31.7	42.4
	Never	479	56.0	57.6	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.10 : I use MXiT to meet new people

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	179	20.9	21.5	21.5
	Some times	342	40.0	41.1	62.6
	Never	311	36.3	37.4	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.11: I don't mind who I talk to in chat rooms

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	128	15.0	15.4	15.4
	Some times	270	31.5	32.5	47.9
	Never	433	50.6	52.1	100.0
	Total	831	97.1	100.0	
Missing	System	25	2.9		
Total		856	100.0		

Question 15.12 : I use MXiT to only chat to people I know

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	399	46.6	48.0	48.0
	Some times	300	35.0	36.1	84.0
	Never	133	15.5	16.0	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 15.13 : If there is abuse on MXiT, I inform my parents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	303	35.4	36.5	36.5
	Some times	197	23.0	23.7	60.2
	Never	331	38.7	39.8	100.0
	Total	831	97.1	100.0	
Missing	System	25	2.9		
Total		856	100.0		

Question 16.1 : Are you aware of the possible dangers in using MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	723	84.5	86.9	86.9
	No	109	12.7	13.1	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 16.2 : Are you aware that criminals can use fake IDs and pretend to be somebody they are not ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	737	86.1	88.6	88.6
	No	95	11.1	11.4	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 16.3 : Do you know that people can get addicted to MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	762	89.0	91.6	91.6
	No	70	8.2	8.4	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Question 16.4 : Have you heard of examples where people have got abducted because of the contacts then have met using MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	629	73.5	75.6	75.6
	No	203	23.7	24.4	100.0
	Total	832	97.2	100.0	
Missing	System	24	2.8		
Total		856	100.0		

Parents

Name of District where School is Located

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Umlazi	380	50.6	50.6	50.6
	Pinetown	234	31.2	31.2	81.8
	ILembe	137	18.2	18.2	100.0
	Total	751	100.0	100.0	

Respondent Highest Qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Tertiary	295	39.3	39.3	39.3
	Matric	209	27.8	27.8	67.1
	Other	247	32.9	32.9	100.0
	Total	751	100.0	100.0	

Respondent Ethnic Group

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	African	187	24.9	24.9	24.9
	Coloured	29	3.9	3.9	28.8
	Asian	458	61.0	61.0	89.7
	White	29	3.9	3.9	93.6
	Other	48	6.4	6.4	100.0
	Total	751	100.0	100.0	

Question 3.1 : Do you own a mobile cellular phone ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	657	87.5	87.5	87.5
	No	94	12.5	12.5	100.0
	Total	751	100.0	100.0	

Question 3.2 : Have you heard of what MXiT is ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	722	96.1	96.1	96.1
	No	29	3.9	3.9	100.0
	Total	751	100.0	100.0	

Question 3.3 : Are you aware of whether your child/children are using MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	548	73.0	73.0	73.0
	No	203	27.0	27.0	100.0
	Total	751	100.0	100.0	

Question 3.4 : Has your child ever asked for permission to use MXiT ?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	282	37.5	37.5	37.5
	No	469	62.5	62.5	100.0
	Total	751	100.0	100.0	

Question 3.5.1 : Age Restrictions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	467	62.2	62.2	62.2
	No	284	37.8	37.8	100.0
	Total	751	100.0	100.0	

Question 3.5.2 : Parents being able to block chatrooms on MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	397	52.9	52.9	52.9
	No	354	47.1	47.1	100.0
	Total	751	100.0	100.0	

Question 3.5.3 : Being able to report abuse using MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	445	59.3	59.3	59.3
	No	306	40.7	40.7	100.0
	Total	751	100.0	100.0	

Question 3.6.1 : Addiction, and children getting addicted to MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	680	90.5	90.5	90.5
	No	71	9.5	9.5	100.0
	Total	751	100.0	100.0	

Question 3.6.2 : Criminals using fake IDs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	620	82.6	82.6	82.6
	No	131	17.4	17.4	100.0
	Total	751	100.0	100.0	

Question 3.6.3 : Communicating with strangers on MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	686	91.3	91.3	91.3
	No	65	8.7	8.7	100.0
	Total	751	100.0	100.0	

Question 3.6.4 : Abduction of children that have been using MXiT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	613	81.6	81.6	81.6
	No	138	18.4	18.4	100.0
	Total	751	100.0	100.0	

Appendix G : Dispersion Statistics Cross Tabulations

Ethnic Group

Name of the District where school is located * Respondent Ethnic Group Crosstabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
D1: Name of the District where school is located	ILembe	9.1%	1.3%	9.1%	.1%	.1%	19.7%
	Pinetown	20.3%	.9%	16.8%		.1%	38.2%
	Umlazi	10.5%	1.6%	26.9%	2.0%	1.1%	42.1%
Total		40.0%	3.9%	52.8%	2.1%	1.3%	100.0%

Age group of respondent * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
B1: Age group of respondent	12 -13 yrs	3.4%	.5%	12.1%	.5%	.6%	17.1%
	14 - 15 yrs	13.1%	2.5%	23.8%	1.1%	.6%	41.0%
	16 - 17 yrs	18.5%	.6%	16.2%	.5%	.1%	35.9%
	18 - 20 yrs	5.0%	.4%	.6%	.1%		6.1%
Total		40.0%	3.9%	52.8%	2.1%	1.3%	100.0%

Gender of the respondent * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
B2 : Gender of the respondent	Male	15.7%	2.2%	21.7%	1.6%	.7%	41.9%
	Female	24.3%	1.6%	31.1%	.5%	.6%	58.1%
Total		40.0%	3.9%	52.8%	2.1%	1.3%	100.0%

Respondent Studying Grade * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
B3: Respondent Studying Grade	Grade 8	7.2%	.7%	11.9%	.7%	.4%	20.9%
	Grade 9	9.1%	1.9%	17.6%	.6%	.8%	30.0%
	Grade 10	11.4%	.5%	13.3%	.1%	.1%	25.5%
	Grade 11	12.1%	.8%	9.9%	.7%		23.6%
Total		40.0%	3.9%	52.8%	2.1%	1.3%	100.0%

5.1: I have my own mobile cellular phone * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S5.1: I have my own mobile cellular phone	Yes	27.0%	3.6%	45.2%	2.1%	.9%	78.9%
	No	13.0%	.2%	7.6%		.4%	21.1%
Total		40.0%	3.9%	52.8%	2.1%	1.3%	100.0%

5.2: I have heard about and use MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S5.2: I have heard about and use MXiT	Yes	35.9%	3.6%	49.5%	2.1%	1.1%	92.2%
	No	4.1%	.2%	3.3%		.2%	7.8%
Total		40.0%	3.9%	52.8%	2.1%	1.3%	100.0%

6: I have been using MXIT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S6: I have been using MXIT	For years	10.8%	1.8%	27.2%	1.8%	.5%	42.1%
	For about the last year	11.4%	1.4%	13.3%	.1%	.5%	26.7%
	For less than 6 Months	8.0%	.5%	5.7%	.4%		14.6%
	For the Last month only	8.7%	.3%	7.5%		.1%	16.6%
	Total	38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

7 : I Use MXiT mainly from * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S7 : I Use MXiT mainly from	My Own mobile phone	24.6%	3.4%	44.7%	2.3%	.8%	75.8%
	A friend's mobile phone	7.1%	.3%	2.5%		.1%	10.0%
	My parents mobile phone	5.3%	.1%	3.7%		.1%	9.3%
	Other	1.9%	.1%	2.8%		.1%	4.9%
	Total	38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

8 : I use MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S8 : I use MXIT	Every day	15.6%	1.9%	27.9%	.9%	.5%	46.8%
	At least 3 times a week	9.9%	.8%	10.6%	1.1%	.3%	22.7%
	At least once per week	6.5%	1.0%	6.3%	.1%	.1%	14.1%
	Less than once per week	7.0%	.3%	8.9%	.1%	.3%	16.5%
	Total	38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

9 : I normally use MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S9 : I normally use MXiT	Anytime day or night	11.8%	1.5%	19.8%	.8%		33.8%
	Only on weekends	12.0%	.9%	11.3%	.1%	.3%	24.6%
	Only during school hours	.5%	.1%	.3%			.9%
	Anytime but not during school hours	14.6%	1.4%	22.4%	1.4%	.9%	40.7%
	Total	38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

10: I am most likely to use MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S10: I am most likely to use MXiT	Only when I am alone	21.9%	2.0%	22.4%	1.3%	.3%	47.9%
	When I am around friends	5.7%	.1%	6.1%		.1%	12.0%
	When I am around friends or family	7.5%	1.1%	16.1%	.5%	.5%	25.7%
	Not when I am around family	3.8%	.6%	9.1%	.5%	.3%	14.3%
	Total	38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

11: When I use MXiT, it is normally * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S11: When I use MXiT, it is normally	To send important messeges only	4.2%	.1%	4.1%	.5%	.3%	9.1%
	To socialise and chat to my friends	20.4%	2.9%	39.1%	1.5%	.8%	64.7%
	To communicate with my family	1.0%		3.0%			4.1%
	Because I am bored	13.3%	.9%	7.5%	.3%	.1%	22.1%
	Total	39.0%	3.9%	53.7%	2.3%	1.1%	100.0%

12: When I use MXiT, it is normally * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S12: When I use MXiT, it is normally	Less than 5 mins	4.1%	.4%	3.7%	.1%	.5%	8.7%
	Less than 15 mins	5.2%	.5%	7.5%	.6%	.1%	13.9%
	Less than 30 mins	7.0%	.3%	12.4%	1.0%	.1%	20.8%
	At least for an hour	22.7%	2.8%	30.2%	.5%	.4%	56.5%
Total		38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

13: I use MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S13: I use MXiT	For using the cheap message service	15.3%	1.8%	37.3%	2.2%	.8%	57.3%
	Only for the chatrooms	4.6%	.8%	1.3%			6.6%
	To send and receive music / pics	5.1%	.1%	2.2%			7.4%
	All of the above	13.9%	1.3%	13.1%	.1%	.4%	28.8%
Total		38.9%	3.9%	53.7%	2.3%	1.1%	100.0%

14.1: I use MXiT chat rooms * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.1: I use MXiT chat rooms	Yes	20.1%	.7%	9.4%	.6%	.1%	31.0%
	No	20.0%	3.1%	43.3%	1.6%	1.1%	69.0%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.2: Are you aware of the rules that exist in using MXIT chat rooms * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.2: Are you aware of the rules that exist in using MXIT chat rooms	Yes	23.8%	3.0%	39.0%	1.4%	.7%	67.9%
	No	16.3%	.8%	13.8%	.7%	.5%	32.1%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.3: When entering chat rooms, are you warned about keeping your personal information private * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.3: When entering chat rooms, are you warned about keeping your personal information private	Yes	27.1%	2.8%	41.9%	1.8%	.7%	74.3%
	No	12.9%	1.1%	10.9%	.4%	.5%	25.7%
Total		40.0%	3.8%	52.8%	2.2%	1.2%	100.0%

14.4: Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.4: Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details	Yes	12.4%	1.2%	17.2%	.8%	.4%	32.1%
	No	27.6%	2.6%	35.5%	1.3%	.8%	67.9%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.5: Have you shared your cell phone password with friends or anyone else * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.5: Have you shared your cell phone password with friends or anyone else	Yes	8.7%	.5%	9.7%			18.9%
	No	31.3%	3.3%	43.1%	2.2%	1.2%	81.1%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.6: Have you shared your MXIT pin with friends or anyone else * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.6: Have you shared your MXIT pin with friends or anyone else	Yes	9.3%	.7%	10.4%	.2%	.1%	20.8%
	No	30.7%	3.1%	42.3%	1.9%	1.1%	79.2%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.7: Using MXiT, have you communicated with people you have not met and do not know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.7: Using MXiT, have you communicated with people you have not met and do not know	Yes	28.7%	2.5%	25.5%	.2%	.5%	57.4%
	No	11.4%	1.3%	27.3%	1.9%	.7%	42.6%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.8: Have you ever opened a picture sent from somebody you do not know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.8: Have you ever opened a picture sent from somebody you do not know	Yes	23.0%	2.0%	23.3%	.6%	.2%	49.2%
	No	17.1%	1.8%	29.4%	1.6%	1.0%	50.8%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.9: Have you ever met anyone in person that you have met online * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.9: Have you ever met anyone in person that you have met online	Yes	16.5%	1.6%	20.0%	.7%	.4%	39.1%
	No	23.6%	2.3%	32.8%	1.4%	.8%	60.9%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.10: Have you ever considered meeting anyone in person that you have met online, and then changed your mind? * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.10: Have you ever considered meeting anyone in person that you have met online, and then changed your mind?	Yes	16.6%	1.6%	13.4%	.2%	.4%	32.2%
	No	23.5%	2.3%	39.3%	1.9%	.8%	67.8%
Total		40.1%	3.8%	52.7%	2.2%	1.2%	100.0%

14.11: Have you informed your parents that you have registered on MXIT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.11: Have you informed your parents that you have registered on MXIT	Yes	14.4%	2.3%	37.9%	2.0%	.7%	57.3%
	No	25.7%	1.6%	14.8%	.1%	.5%	42.7%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.12: Are you aware that chat rooms have moderators that monitor the conversation * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.12: Are you aware that chat rooms have moderators that monitor the conversation	Yes	15.1%	1.4%	27.5%	1.0%	.6%	45.6%
	No	25.0%	2.4%	25.2%	1.2%	.6%	54.4%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.13: Are you aware of the .rat command to report abuse on MXIT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S14.13: Are you aware of the .rat command to report abuse on MXIT	Yes	17.6%	2.8%	31.7%	1.1%	.6%	53.7%
	No	22.5%	1.1%	21.1%	1.1%	.6%	46.3%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

14.14: Are you aware that you can set up your own chatroom, and can limit this only to people you know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S14.14: Are you aware that you can set up your own chatroom, and can limit this only to people you know	Yes	24.8%	3.2%	39.8%	1.6%	1.1%	70.5%
	No	15.3%	.6%	12.9%	.6%	.1%	29.5%
Total		40.1%	3.8%	52.8%	2.2%	1.2%	100.0%

15.1: The use of MXIT can be dangerous and open to abuse * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.1: The use of MXIT can be dangerous and open to abuse	Always	6.6%	1.1%	11.7%	.2%	.5%	20.1%
	Some times	28.7%	2.4%	38.7%	1.3%	.6%	71.8%
	Never	4.7%	.2%	2.5%	.6%	.1%	8.2%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.2: My cell phone password is kept secret at all times * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.2: My cell phone password is kept secret at all times	Always	26.6%	2.6%	43.4%	2.2%	1.1%	75.8%
	Some times	8.5%	1.0%	8.3%		.1%	17.9%
	Never	4.9%	.1%	1.2%			6.3%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.3: My MXIT password is important to keep confidential * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.3: My MXIT password is important to keep confidential	Always	27.5%	3.4%	47.8%	1.9%	1.1%	81.7%
	Some times	7.7%	.2%	3.4%	.2%	.1%	11.7%
	Never	4.8%	.1%	1.7%			6.6%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.4: MXIT is fun and is not dangerous at all * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.4: MXIT is fun and is not dangerous at all	Always	5.2%	.5%	9.9%	.7%	.1%	16.3%
	Some times	25.8%	2.9%	36.2%	1.3%	.6%	66.8%
	Never	9.0%	.4%	6.9%	.1%	.5%	16.8%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.5: I only use MXIT to talk to people I know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.5: I only use MXIT to talk to people I know	Always	10.7%	1.8%	30.7%	1.8%	.7%	45.7%
	Some times	18.7%	1.6%	19.0%	.4%	.2%	39.8%
	Never	10.6%	.4%	3.2%		.2%	14.4%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.6: I talk to strangers on MXIT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.6: I talk to strangers on MXIT	Always	7.6%	.6%	2.9%	.1%	.1%	11.3%
	Some times	17.9%	1.3%	18.0%	.4%	.5%	38.1%
	Never	14.5%	1.8%	32.0%	1.7%	.6%	50.6%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.7: I download files from people I do not know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.7: I download files from people I do not know	Always	4.2%	.5%	2.5%	.1%	.2%	7.6%
	Some times	13.8%	.8%	10.8%	.2%	.2%	26.0%
	Never	22.0%	2.4%	39.5%	1.8%	.7%	66.5%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.8: I send pictures to people I do not know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.8: I send pictures to people I do not know	Always	2.4%	.1%	1.8%	.1%		4.4%
	Some times	9.3%	1.0%	7.1%	.2%	.4%	17.9%
	Never	28.4%	2.6%	44.0%	1.8%	.8%	77.6%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.9: I have online friendships or relationships with people I have not met * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.9: I have online friendships or relationships with people I have not met	Always	7.3%	.4%	2.9%	.1%		10.7%
	Some times	16.6%	1.2%	13.2%	.2%	.5%	31.7%
	Never	16.1%	2.2%	36.8%	1.8%	.7%	57.6%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

S15.10: I use MXiT to meet new people * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.10: I use MXiT to meet new people	Always	12.3%	1.0%	7.9%	.2%	.1%	21.5%
	Some times	16.7%	1.7%	21.9%	.2%	.6%	41.1%
	Never	11.1%	1.1%	23.1%	1.7%	.5%	37.4%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.11: I don't mind who I talk to in chat rooms * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.11: I don't mind who I talk to in chat rooms	Always	7.7%	1.2%	5.7%	.6%	.2%	15.4%
	Some times	18.5%	1.0%	12.8%		.2%	32.5%
	Never	13.7%	1.6%	34.5%	1.6%	.7%	52.1%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.12: I use MXIT to only chat to people I know * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.12: I use MXIT to only chat to people I know	Always	10.9%	1.6%	33.2%	1.7%	.6%	48.0%
	Some times	18.0%	1.4%	15.7%	.4%	.5%	36.1%
	Never	11.1%	.7%	4.0%	.1%	.1%	16.0%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

15.13: If there is abuse on MXIT, I inform my parents * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S15.13: If there is abuse on MXIT, I inform my parents	Always	10.5%	1.2%	23.0%	1.2%	.6%	36.5%
	Some times	7.3%	1.0%	14.3%	.6%	.5%	23.7%
	Never	22.3%	1.6%	15.5%	.4%	.1%	39.8%
Total		40.1%	3.7%	52.8%	2.2%	1.2%	100.0%

16.1: Are you aware of the possible dangers in using MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					Total
		African	Coloured	Asian	White	Other	
S16.1: Are you aware of the possible dangers in using MXiT	Yes	29.9%	3.5%	50.5%	1.9%	1.1%	86.9%
	No	10.1%	.2%	2.4%	.2%	.1%	13.1%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

16.2: Are you aware that criminals can use fake IDs and pretend to be someone they are not * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S16.2: Are you aware that criminals can use fake IDs and pretend to be someone they are not	Yes	31.9%	2.9%	50.7%	2.2%	1.0%	88.6%
	No	8.2%	.8%	2.2%		.2%	11.4%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

16.3: Do you know that people can get addicted to MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S16.3: Do you know that people can get addicted to MXiT	Yes	33.7%	3.6%	51.3%	1.8%	1.2%	91.6%
	No	6.4%	.1%	1.6%	.4%		8.4%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

16.4: Have you heard of examples where people have got abducted because of the contacts they have met using MXiT * Respondent Ethnic Group Cross tabulation

% of Total

		B4: Respondent Ethnic Group					
		African	Coloured	Asian	White	Other	Total
S16.4: Have you heard of examples where people have got abducted because of the contacts they have met using MXiT	Yes	23.0%	3.0%	47.5%	1.2%	1.0%	75.6%
	No	17.1%	.7%	5.4%	1.0%	.2%	24.4%
Total		40.0%	3.7%	52.9%	2.2%	1.2%	100.0%

Age

Name of the District where school is located * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
D1: Name of the District where school is located	ILembe	3.2%	8.4%	7.5%	.7%	19.7%
	Pinetown	6.1%	11.7%	16.7%	3.7%	38.2%
	Umlazi	7.8%	20.9%	11.7%	1.6%	42.1%
Total		17.1%	41.0%	35.9%	6.1%	100.0%

Gender of the respondent * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
B2 : Gender of the respondent	Male	7.8%	15.3%	15.3%	3.5%	41.9%
	Female	9.2%	25.7%	20.6%	2.6%	58.1%
Total		17.1%	41.0%	35.9%	6.1%	100.0%

Respondent Studying Grade * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
B3: Respondent Studying Grade	Grade 8	15.0%	5.7%	.1%	.1%	20.9%
	Grade 9	2.1%	25.1%	2.7%	.1%	30.0%
	Grade 10		9.5%	14.8%	1.2%	25.5%
	Grade 11		.7%	18.2%	4.7%	23.6%
Total		17.1%	41.0%	35.9%	6.1%	100.0%

Respondent Ethnic Group * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
B4: Respondent Ethnic Group	African	3.4%	13.1%	18.5%	5.0%	40.0%
	Coloured	.5%	2.5%	.6%	.4%	3.9%
	Asian	12.1%	23.8%	16.2%	.6%	52.8%
	White	.5%	1.1%	.5%	.1%	2.1%
	Other	.6%	.6%	.1%		1.3%
Total		17.1%	41.0%	35.9%	6.1%	100.0%

5.1: I have my own mobile cellular phone * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S5.1: I have my own mobile cellular phone	Yes	12.5%	32.8%	28.7%	4.8%	78.9%
	No	4.6%	8.2%	7.1%	1.3%	21.1%
Total		17.1%	41.0%	35.9%	6.1%	100.0%

5.2: I have heard about and use MXiT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S5.2: I have heard about and use MXiT	Yes	14.1%	37.7%	34.3%	6.0%	92.2%
	No	2.9%	3.3%	1.5%	.1%	7.8%
Total		17.1%	41.0%	35.9%	6.1%	100.0%

6: I have been using MXIT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S6: I have been using MXIT	For years	3.5%	17.5%	19.0%	2.0%	42.1%
	For about the last year	4.6%	11.9%	8.2%	2.0%	26.7%
	For less than 6 Months	3.2%	5.2%	4.8%	1.4%	14.6%
	For the Last month only	4.1%	6.3%	5.2%	1.0%	16.6%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

7 : I Use MXiT mainly from * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S7 : I Use MXiT mainly from	My Own mobile phone	11.4%	32.4%	27.5%	4.4%	75.8%
	A friend's mobile phone	1.0%	3.7%	4.4%	0.9%	10.0%
	My parents mobile phone	1.8%	2.9%	4.1%	0.5%	9.3%
	Other	1.1%	1.9%	1.3%	0.6%	4.9%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

8 : I use MXIT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S8 : I use MXIT	Every day	5.3%	21.7%	17.4%	2.4%	46.8%
	At least 3 times a week	3.0%	9.4%	9.0%	1.3%	22.7%
	At least once per week	2.9%	5.3%	4.1%	1.8%	14.1%
	Less than once per week	4.1%	4.6%	6.8%	1.0%	16.5%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

9 : I normally use MXiT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S9 : I normally use MXiT	Anytime day or night	4.1%	15.2%	12.4%	2.2%	33.8%
	Only on weekends	5.8%	10.0%	7.2%	1.5%	24.6%
	Only during school hours		0.4%	0.5%		0.9%
	Anytime but not during school hours	5.4%	15.3%	17.1%	2.8%	40.7%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

10: I am most likely to use MXiT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S10: I am most likely to use MXiT	Only when I am alone	5.1%	19.0%	19.8%	4.1%	47.9%
	When I am around friends	2.3%	4.3%	4.4%	1.0%	12.0%
	When I am around friends or family	5.1%	11.5%	8.2%	0.9%	25.7%
	Not when I am around family	2.9%	6.1%	4.8%	0.5%	14.3%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

11: When I use MXiT, it is normally * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S11: When I use MXiT, it is normally	To send important messeges only	1.5%	3.9%	3.0%	0.6%	9.1%
	To socialise and chat to my friends	9.9%	27.9%	23.1%	3.8%	64.7%
	To communicate with my family	1.4%	1.4%	1.1%	0.1%	4.1%
	Because I am bored	2.5%	7.7%	9.9%	1.9%	22.1%
Total		15.4%	41.0%	37.2%	6.5%	100.0%

12: When I use MXiT, it is normally * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S12: When I use MXiT, it is normally	Less than 5 mins	1.4%	3.8%	3.4%	0.1%	8.7%
	Less than 15 mins	4.7%	5.4%	2.7%	1.1%	13.9%
	Less than 30 mins	3.7%	8.4%	7.7%	1.0%	20.8%
	At least for an hour	5.6%	23.3%	23.4%	4.2%	56.5%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

13: I use MXiT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S13: I use MXiT	For using the cheap message service	9.4%	24.6%	20.2%	3.2%	57.3%
	Only for the chatrooms	1.4%	2.7%	1.5%	1.0%	6.6%
	To send and receive music / pics	1.9%	3.3%	2.2%		7.4%
	All of the above	2.7%	10.4%	13.4%	2.3%	28.8%
Total		15.3%	40.9%	37.3%	6.5%	100.0%

14.1: I use MXiT chat rooms * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S14.1: I use MXiT chat rooms	Yes	3.3%	8.7%	15.1%	3.8%	31.0%
	No	12.9%	32.8%	21.1%	2.3%	69.0%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.2: Are you aware of the rules that exist in using MXIT chat rooms * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.2: Are you aware of the rules that exist in using MXIT chat rooms	Yes	11.0%	26.6%	26.2%	4.2%	67.9%
	No	5.3%	15.0%	9.9%	1.9%	32.1%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.3: When entering chat rooms, are you warned about keeping your personal information private * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.3: When entering chat rooms, are you warned about keeping your personal information private	Yes	10.4%	30.2%	29.2%	4.4%	74.3%
	No	5.9%	11.3%	6.9%	1.7%	25.7%
Total		16.3%	41.4%	36.2%	6.1%	100.0%

14.4: Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.4: Have you ever revealed personal information on MXIT previously, for eg. your real name, telephone number, home address, or any other personal details	Yes	3.2%	13.3%	13.3%	2.3%	32.1%
	No	13.0%	28.2%	22.8%	3.8%	67.9%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.5: Have you shared your cell phone password with friends or anyone else * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.5: Have you shared your cell phone password with friends or anyone else	Yes	1.9%	7.4%	8.3%	1.3%	18.9%
	No	14.4%	34.1%	27.9%	4.8%	81.1%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.6: Have you shared your MXIT pin with friends or anyone else * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.6: Have you shared your MXIT pin with friends or anyone else	Yes	2.2%	8.0%	9.4%	1.2%	20.8%
	No	14.1%	33.5%	26.7%	4.9%	79.2%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.7: Using MXiT, have you communicated with people you have not met and do not know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.7: Using MXiT, have you communicated with people you have not met and do not know	Yes	5.0%	22.5%	25.4%	4.5%	57.4%
	No	11.2%	19.0%	10.8%	1.6%	42.6%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.8: Have you ever opened a picture sent from somebody you do not know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S14.8: Have you ever opened a picture sent from somebody you do not know	Yes	4.1%	18.3%	22.7%	4.1%	49.2%
	No	12.2%	23.2%	13.4%	2.0%	50.8%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.9: Have you ever met anyone in person that you have met online * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S14.9: Have you ever met anyone in person that you have met online	Yes	6.2%	14.2%	15.7%	3.0%	39.1%
	No	10.0%	27.3%	20.5%	3.1%	60.9%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.10: Have you ever considered meeting anyone in person that you have met online, and then changed your mind? * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S14.10: Have you ever considered meeting anyone in person that you have met online, and then changed your mind?	Yes	4.0%	10.2%	15.3%	2.8%	32.2%
	No	12.2%	31.4%	20.8%	3.4%	67.8%
Total		16.2%	41.6%	36.2%	6.1%	100.0%

14.11: Have you informed your parents that you have registered on MXIT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.11: Have you informed your parents that you have registered on MXIT	Yes	10.2%	24.9%	19.6%	2.6%	57.3%
	No	6.1%	16.6%	16.5%	3.5%	42.7%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.12: Are you aware that chat rooms have moderators that monitor the conversation * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.12: Are you aware that chat rooms have moderators that monitor the conversation	Yes	6.9%	20.5%	15.3%	2.9%	45.6%
	No	9.3%	21.1%	20.8%	3.2%	54.4%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.13: Are you aware of the .rat command to report abuse on MXIT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.13: Are you aware of the .rat command to report abuse on MXIT	Yes	9.4%	21.8%	19.0%	3.5%	53.7%
	No	6.8%	19.7%	17.1%	2.6%	46.3%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

14.14: Are you aware that you can set up your own chatroom, and can limit this only to people you know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S14.14: Are you aware that you can set up your own chatroom, and can limit this only to people you know	Yes	10.9%	29.4%	26.3%	3.8%	70.5%
	No	5.4%	12.1%	9.8%	2.3%	29.5%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.1: The use of MXIT can be dangerous and open to abuse * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.1: The use of MXIT can be dangerous and open to abuse	Always	4.6%	8.5%	5.9%	1.1%	20.1%
	Some times	10.9%	28.6%	27.9%	4.3%	71.8%
	Never	.8%	4.3%	2.3%	.7%	8.2%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.2: My cell phone password is kept secret at all times * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.2: My cell phone password is kept secret at all times	Always	13.6%	32.0%	25.6%	4.7%	75.8%
	Some times	2.3%	7.0%	7.7%	1.0%	17.9%
	Never	.5%	2.5%	2.8%	.5%	6.3%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.3: My MXIT password is important to keep confidential * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.3: My MXIT password is important to keep confidential	Always	14.3%	34.4%	28.4%	4.7%	81.7%
	Some times	1.4%	3.7%	5.4%	1.1%	11.7%
	Never	.6%	3.4%	2.3%	.4%	6.6%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.4: MXIT is fun and is not dangerous at all * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.4: MXIT is fun and is not dangerous at all	Always	2.2%	6.3%	7.5%	.5%	16.3%
	Some times	10.9%	28.6%	22.8%	4.4%	66.8%
	Never	3.2%	6.6%	5.8%	1.2%	16.8%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.5: I only use MXIT to talk to people I know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.5: I only use MXIT to talk to people I know	Always	10.5%	20.1%	13.1%	2.0%	45.7%
	Some times	4.9%	14.3%	17.0%	3.6%	39.8%
	Never	1.0%	7.0%	6.0%	.5%	14.4%
Total		16.4%	41.4%	36.1%	6.1%	100.0%

15.6: I talk to strangers on MXIT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.6: I talk to strangers on MXIT	Always	1.0%	3.1%	6.1%	1.1%	11.3%
	Some times	3.7%	13.8%	17.3%	3.2%	38.1%
	Never	11.7%	24.5%	12.6%	1.8%	50.6%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.7: I download files from people I do not know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.7: I download files from people I do not know	Always	.8%	2.6%	3.5%	.6%	7.6%
	Some times	2.3%	9.3%	11.5%	2.9%	26.0%
	Never	13.2%	29.6%	21.0%	2.6%	66.5%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.8: I send pictures to people I do not know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.8: I send pictures to people I do not know	Always	.5%	2.3%	1.6%	.1%	4.4%
	Some times	1.8%	5.2%	8.7%	2.3%	17.9%
	Never	14.1%	34.0%	25.8%	3.7%	77.6%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.9: I have online friendships or relationships with people I have not met * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.9: I have online friendships or relationships with people I have not met	Always	.8%	3.4%	5.2%	1.3%	10.7%
	Some times	3.8%	11.2%	14.1%	2.6%	31.7%
	Never	11.7%	26.9%	16.8%	2.2%	57.6%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.10: I use MXiT to meet new people * Age group of respondent Crosstabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.10: I use MXiT to meet new people	Always	2.5%	7.3%	9.7%	1.9%	21.5%
	Some times	5.5%	15.5%	17.4%	2.6%	41.1%
	Never	8.3%	18.6%	8.9%	1.6%	37.4%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.11: I don't mind who I talk to in chat rooms * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.11: I don't mind who I talk to in chat rooms	Always	2.4%	5.1%	6.4%	1.6%	15.4%
	Some times	4.5%	11.3%	14.1%	2.6%	32.5%
	Never	9.5%	25.2%	15.5%	1.9%	52.1%
Total		16.4%	41.5%	36.0%	6.1%	100.0%

15.12: I use MXIT to only chat to people I know * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S15.12: I use MXIT to only chat to people I know	Always	10.9%	21.8%	13.3%	1.9%	48.0%
	Some times	4.2%	13.9%	14.7%	3.2%	36.1%
	Never	1.2%	5.8%	8.1%	1.0%	16.0%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

15.13: If there is abuse on MXIT, I inform my parents * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S15.13: If there is abuse on MXIT, I inform my parents	Always	9.9%	16.1%	9.4%	1.1%	36.5%
	Some times	4.1%	10.2%	8.4%	1.0%	23.7%
	Never	2.4%	15.2%	18.2%	4.1%	39.8%
Total		16.4%	41.5%	36.0%	6.1%	100.0%

16.1: Are you aware of the possible dangers in using MXiT * Age group of respondent Cross tabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S16.1: Are you aware of the possible dangers in using MXiT	Yes	14.8%	35.1%	31.6%	5.4%	86.9%
	No	1.6%	6.4%	4.4%	.7%	13.1%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

16.2: Are you aware that criminals can use fake IDs and pretend to be someone they are not * Age group of respondent Crosstabulation

% of Total

		B1: Age group of respondent				Total
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	
S16.2: Are you aware that criminals can use fake IDs and pretend to be someone they are not	Yes	15.0%	35.5%	32.5%	5.6%	88.6%
	No	1.3%	6.0%	3.6%	.5%	11.4%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

16.3: Do you know that people can get addicted to MXiT * Age group of respondent Crosstabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S16.3: Do you know that people can get addicted to MXiT	Yes	15.4%	37.5%	33.5%	5.2%	91.6%
	No	1.0%	4.0%	2.5%	1.0%	8.4%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

16.4: Have you heard of examples where people have got abducted because of the contacts they have met using MXiT * Age group of respondent Crosstabulation

% of Total

		B1: Age group of respondent				
		12 -13 yrs	14 - 15 yrs	16 - 17 yrs	18 - 20 yrs	Total
S16.4: Have you heard of examples where people have got abducted because of the contacts they have met using MXiT	Yes	13.5%	31.5%	26.6%	4.1%	75.6%
	No	2.9%	10.0%	9.5%	2.0%	24.4%
Total		16.3%	41.5%	36.1%	6.1%	100.0%

Appendix H : Ethical Clearance Letters

UNIVERSITY OF
KWAZULU-NATAL

University of KwaZulu-Natal
Research Office
Govan Mbeki Centre
Westville Campus
University Road
Westville
4000
South Africa
Tel No: +27 31 260 3587
Fax No: +27 31 260 4609

24 FEBRUARY 2010

Mrs. N Bhoola
School of IS & T
WESTVILLE CAMPUS

Dear Mrs. Bhoola

ETHICAL APPROVAL NUMBER: HSS/1092/10M
PROJECT TITLE: "An investigation of High School Learners using MIXit, and their Attitudes towards Mobile Security Framework"

In response to your application dated 22 February 2010, Student Number: **9038406** the Humanities & Social Sciences Ethics Committee has considered the abovementioned application and the protocol has been given **FULL APPROVAL.**

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study must be reviewed and approved through the amendment /modification prior to its implementation. Please quote the above reference number for all queries relating to this study.
PLEASE NOTE: Research data should be securely stored in the school/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Professor Steve Collings (Chair)
HUMANITIES & SOCIAL SCIENCES ETHICS COMMITTEE

cc. Supervisor (Professor M Maharaj)
cc. Mrs. C Haddon

PROVINCE OF KWAZULU-NATAL
ISIFUNDAZWE SAKWAZULU-NATALI

DEPARTMENT OF EDUCATION
UMNYANGO WEMFUNDO

Tel: 033 341 8610
Fax: 033 341 8612
Private Bag X9137
Pietermaritzburg
3200

228 Pietermaritz Street
PIETERMARITZBURG

INHLOKOHOVISI | PIETERMARITZBURG | HEAD OFFICE

Imibuzo: Enquiries: Sibusiso Alwar | Reference: Inkomba: 0073/2009 | Date: Usuku: 02 November 2009

MRS N BHOOLA
PO BOX 15
HYPER BY THE SEA
DURBAN
4053

PERMISSION TO INTERVIEW LEARNERS AND EDUCATORS

The above matter refers.

Permission is hereby granted to interview Departmental Officials, learners and educators in selected schools of the Province of KwaZulu-Natal subject to the following conditions:

1. **You make all the arrangements concerning your interviews.**
2. **Educators' programmes are not interrupted.**
3. **Interviews are not conducted during the time of writing examinations in schools.**
4. **Learners, educators and schools are not identifiable in any way from the results of the interviews.**
5. **Your interviews are limited only to targeted schools.**
6. **A brief summary of the interview content, findings and recommendations is provided to my office.**
7. **A copy of this letter is submitted to District Managers and principals of schools where the intended interviews are to be conducted.**

The KZN Department of education fully supports your commitment to research: **An investigation of high school learners using MXIT, and their attitudes towards mobile security frameworks**

It is hoped that you will find the above in order.

Best Wishes

R Cassius Lubisi, (PhD)
Superintendent-General