Risks: Hacking, Identity Theft and Burglary that are associated with students (aged 18-24) in sharing personal data through Social Media Applications.

A dissertation submitted in partial fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Business Information Systems.

By Benjamin Donoghue

Department of Computing & Information Systems
Cardiff School of Management

Cardiff Metropolitan University

April 2017
DECLARATION

I hereby declare that this dissertation entitled *Risks: Hacking, Identity Theft and Burglary that are associated with students (aged 18-24) in sharing personal data through social media applications* is entirely my own work, and it has never been submitted nor is it being submitted for any other degree.

Candidate: Benjamin Donoghue
Signature: B.Donoghue
Date: 21/04/2017

Supervisor: Stuart McNeil
Signature:
Abstract

As social media sites like Facebook, Twitter and Instagram are becoming more popular, so does the increase in users. With more individuals joining these sites, the associated risks will rise. This study will research the possible risks; hacking, identity theft and burglary that can occur from using these sites, but also examines the student’s awareness of these and investigating views on which social media they think is the least secure.

To get a better understanding of this, the exploration will firstly discover the relevant literature that will be reviewed. It will be in relation to this study, focussing on the use of social media, the advantages, the risks; hacking, identity theft and burglary along with other discussed risks and a brief explanation on the improving the security on social media. This will then follow onto the methodology chapter, where it details the primary research that has been undertaken which are: questionnaires and semi-structured interviews. These will then be analysed and results will be detailed in chapter four. After this will then follow onto chapter five, the discussion, this is where any correlations will be made between primary research and the secondary research.

The overall findings suggests that although students are frequent users of social media, with all having an account, they also agree that hacking, identity theft and burglary can be caused from sharing personal data on these networking sites and they are also aware of the these risks and other dangers. However, in contrast to these results, the majority have never changed their passwords on their accounts and the majority have changed their privacy settings, which links well with the majority stating that Facebook is the least secure social media site, implying and confirming that this site displays the most personal information.
Acknowledgments

Firstly, I would like to thank my supervisor, Stuart McNeil, for his helpfulness and support, especially at the beginning of my project.

Would also like to thank all of the participants who took their time to fill out the questionnaire and special thanks to the four students who took their time in participating in the interviews.

Finally, would like to thank my family and mates for the continuous support and keeping me positive throughout this study.
# Table of Contents

## CHAPTER ONE: INTRODUCTION

1.0 Main Introduction ........................................................................................................... 1  
1.2 Aims and Objectives ...................................................................................................... 3  

## CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction .................................................................................................................. 4  
2.1 The use of Social Media .............................................................................................. 5  
2.2 Advantages of Social Media ...................................................................................... 7  
2.3 The Risks and Security Issues of Social Media ........................................................ 8  
2.3.1 Hacking ................................................................................................................... 8  
2.3.2 Identity Theft ......................................................................................................... 9  
2.3.4 Burglary ................................................................................................................ 10  
2.4 Other Possible Risks ................................................................................................. 11  
2.4.1 Cyber Bullying ...................................................................................................... 12  
2.4.2 Phishing ................................................................................................................ 12  
2.5 Improving Security on Social Media ........................................................................ 13  
2.6 Summary ................................................................................................................... 14  

## CHAPTER THREE: METHODOLOGY

3.0 Introduction .................................................................................................................. 16  
3.1 Research Design .......................................................................................................... 17  
3.2 Samples ....................................................................................................................... 17  
3.3 Mixed Methods .......................................................................................................... 19  
3.4 Questionnaires .......................................................................................................... 19  
3.4.1 Questionnaire Design ............................................................................................ 20  
3.4.2 Questionnaire Advantages .................................................................................. 21  
3.4.3 Questionnaire Disadvantages ............................................................................ 21  
3.5 Semi-Structured Interviews ...................................................................................... 23  
3.5.1 Semi-Structured Interview Layout .................................................................... 23  
3.6 Ethics ......................................................................................................................... 24  
3.7 Summary ................................................................................................................... 26  

## CHAPTER FOUR: RESULTS

4.0 Introduction .................................................................................................................. 27  
4.1 Questionnaire Results ............................................................................................... 27
List of Table and Figures

Table 4 - Questionnaire Results .................................................................27

Figure 5.1 – Total Number of Respondents Per Age -------------------------- -35
Figure 5.2 – Number of who is a Social Media Member ---------------------- -36
Figure 5.3 – Percentage of those who uses What Type of Social Media ------ -36
Figure 5.4 – Percentage of Which Devices used for Social Media ...............-38
Figure 5.5 – Hours Spent on Social Media a Day---------------------------39
Figure 5.6 – Hours Spent on Mobile Devices ............................................. 39
Figure 5.7 – Respondents Who Check Social Media Accounts in Mornings ----40
Figure 5.8 – Problem With Displaying Information on these Sites .............41
Figure 5.9 – Least and Most Secure Social Media Site ...............................43
Figure 5.10 – Personal Information can cause these Risks .......................44
Figure 5.11 – Percentage of Who has or has not been a Victim of the risks ----46
Figure 5.12 – Percentage who are Aware of Threats and Dangers ...............47
Figure 5.13- Percentage of Who has Changed Privacy Settings ..................49
Figure 5.14 – Percentage of How Often Students Change Passwords ..........51
1.0 Main Introduction

Before social media had an impact on the lives of individuals, it was the industry of computers that took over the world. By the early 2000's, the cost of computers, software and the Internet access decreased, allowing individuals access to the same tools of production used by professionals. (Mandiberg, 2012) However, this trend quickly declined with the new invention of the way individuals communicated. The use and the ways of using the Internet as a medium for connecting people with each other have changed in haste. (Warburton, 2012) This is where social media changed the whole new way of communicating and connecting individuals to others. The rise of social media concentrated on the use of technologies that were less technology-focused and more online communities’ users-focused paying attention to the content they created and shared. (Warburton, 2012)

Golbeck (2015), states, “There are also many types of social media based the features they offer.” This research will be focussing on the social networking sites; Facebook, Twitter and Instagram, each are all networking sites but are different in regards to the features they offer. A social networking site will have a strong emphasis on connecting with other people (friending them or forming a social connection). Most modern social network sites also allow people to post status updates, photos, and other contents. The goal behind this is usually to help people engage with their friends by sharing updates about their lives and links to things online they find interesting. Popular sites in this category include Facebook and LinkedIn. (Golbeck, 2015)

Sharing photos and videos is a common part of social media. The ability to share these types of media is built into most social media sites, but some sites are dedicated to this task. Newer sites like Instagram and others are also drawing populations of users. Micro-blogging, these are blogs that were created in the
late 1990's as a way for people to easily post text online without a lot of technical knowledge. These resembled online diaries, and blogging is still extremely popular. These came about in the late 2000's and on Twitter, the most popular micro-blogging website, people's updated are limited to 140 characters. (Golbeck, 2015)

With so many different types of social media, come many advantages of using them. However, with advantages come disadvantages, these disadvantages pose many in association with the use of these sites. This document will outline, the use of social media between 18-24 year olds, the advantages of using these sites, the possible risks than can occur and improving the security of accounts on social media.

So, relevant literature will be explained, using valuable knowledge from different sources. This follows the chapter of the methodology, discussing the chosen methods used within this document. Thereafter, primary research will be conducted from questionnaires and semi-structured interviews. These will then be analysed along with the discussed literature allowing identifying possible links. Lastly, the conclusion will detail the overall progression of this study, stating whether the aims and objectives have been achieved, summarising the overall identified links, closing with a definite conclusion.
1.2 Aims and Objectives

Aim:

To explore the risks that is associated with the use of social media sites and investigating how aware student’s (18-24 year olds) are of these risks.

Objectives:

1. To critically analyse existing literature from published books and articles in the use of social media and how it has become so popular within today's society.

2. Analytically defining the relevant literature from the use of books and news articles of the possible risks that can be occurred from using these sites.

3. To implement primary research, quantitative (questionnaires) and qualitative (semi-structured interviews) in analysing how aware students are in regards to these risks and which site is the least secure from a student’s perspective.
CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter will explore the appropriate literature in relation to the risks of using social media and the use of social media. Aveyard (2014) states “literature review is the comprehensive study and interpretation of literature that addresses a specific topic.” The study of finding relevant data needs to be definite and examined in order for it to be in relation to the research proposal. Through collecting work from previous literature such as books, articles and studies and integrating them will allow to support the aims and objectives of this study.

Social media is defined as websites and applications that enable users to create and share content or to participate in social networking and social media are web-based and mobile technologies that turn communication into active dialogue (Lawsociety.org, 2015).

Lipschultz (2014) explains “many of the newest are focussed on mobile communication, catering to smartphone and tablet users. This dynamic and evolving nature of technology has helped social media spread in popularity to most of the world.” This follows the high usage in many which, social networking sites are part of our student’s daily lives, and they are experts in using them (Purcell, 2012). Social networking sites and other online collaborative tools have emerged as immensely popular places and share information. All have benefits, ranging from practical (e.g. sharing a business document) to purely social (e.g. communicating with distant friends via Facebook). At the same time, not surprisingly, information sharing poses real threats to user privacy (Zheleva, Terzi and Getoor, 2013). Furthermore, Kizza (2007) explains, “as the level of computer crimes increases on the one hand and our reliance and dependence on computer and telecommunications technology increases on the other, we are becoming more and more susceptible and exposed to cyberspace evils and
insecurity.” It is evident that with social media, it imposes many benefits for individual use and also for business use. Consequently, there are many concerns associated when using social media and these can become problematic, which can affect the lives of its users.

2.1 The use of Social Media

Christopher (2015) states “In 2012, of a total population of 63.7 million, around 33 million adults accessed the Internet everyday, with almost half (48%) using social networking sites such as Facebook and Twitter. This makes the UK the second most prolific users of social media in Europe after the Netherlands.” With the increasing usage of social media, it can be argued that social networking is most common within young adults. This can be clarified with Ofcom.org (2015) declaring that “Young adults aged 16-24 have a more extensive breadth of use of social media and are adopting newer sites and services such as Twitter (40%) and Instagram (35%).” However, it was later detailed by Christopher (2015) “the use of social media is most common among between 18-24 year olds, with 91% of internet users in this group owning a Facebook account.” So although social media is popularly used between the ages of 16-24 year olds, it’s greatest use is among 18-24 year olds.

The extent of social media has grown immensely and has become a big part of the lives of individuals, it continues to grow with all ages but really how many times do young adults check their social media accounts? Ofcom.org (2016) explains “84% of 16-24 year olds with a social media profile visits any social media site or app more than once a day.” Ofcom.org (2015) “Smartphones has continued to increase, they are now the most widely-owned internet-enabled device”. This illustrates that the popularity of smartphones have dominated the lives of individuals especially 16-24 year olds, where 90% of these own one. (Ofcom.org, 2015) Furthermore, Yan (2015) illustrated that “those aged 18-24 checked their mobile almost every 10 minutes.” This may demonstrate in how much of a bad habit and addiction individuals have with social media and their smartphones.
Finally, it is claimed that during the day, 18-24 year olds are among the most enthusiastic of smartphone users. (Deloitte, 2016)
2.2 Advantages of Social Media

The main attraction of social media is to maintain communication with friends and family faster and quicker. White (2016) explains, “Social media can be used as a primary means of communication. Additionally, new social networks linking people who may not have been linked before are created, supported and strengthened.” This expresses that new people can be connected enhancing new friendships and relationships. Stonehouse (2014) states “social media venues have helped level the playing field for those that tend to be more on the shy side.” This can be seen as an advantage in that social media helps a variety of different individuals in different ways.

In regards to information being shared on social media, it can become important in the sense of finding out breaking news immediately and efficiently. Asencio (2015) illustrated that “regardless of unquestionable importance of traditional media, there is a trend where the news will spread through social media much faster”. This can be supported by Wakefield (2016) which found “out of the 18-24 year olds surveyed, 28% cited social media as their main news source, compared with 24% for TV”. Surprisingly, social media has become the modern platform to share news immediately; according to Yeomans (2012) “whenever a disaster occurs you can be sure someone will be close by, camera phone and connected social network account at the ready, to provide breaking news footage”. Furthermore, social media sites and applications such as Facebook have created and implemented new modern features. Dredge (2014) states “Facebook Safety Check will help tell friends you’re safe during disasters”. This new feature is a recent feature that allows Facebook users to select an option “I’m safe” which will be posted on the site for friends and family to see. It was later suggested that “while the feature appears to be focused on natural disasters, it could also be used to other kind of crisis: terrorist attacks, for example.” (Dredge, 2014)
2.3 The Risks and Security Issues of Social Media

Importantly, there are clear concerns in regards with using social media with many risks and issues arising from sharing personal information. Dowland (2014) exemplified this “as social media grows in popularity, so does the level of risk associated with using it – people are sharing more and more information about themselves, which leaves them open to abuse and exploitation.” Additionally, as social media continues to attract new users this makes it easier for more criminal activity to happen, “unfortunately, spammers, hackers, phishers, and others see a medium that they may be to exploit by gaining confidential information.” (Harwood, 2010)

Also, Gov.UK (2011) clarifies “the use of blogs and social networking sites is an area of particular concern as the security of such sites is often not well understood by users. Very often the default security settings allow everyone to see submitted information.”

2.3.1 Hacking

It is understandably that hacking is a major concern within the modern communication networks and can consequently cause major risks to individuals; this can be confirmed as Cross (2013) - explains “hacking social media can have far-reaching implications”. Hackers can target anyone, Johnston (2016) demonstrates that “Zuckerberg’s social media accounts targeted by hackers. He might run the worlds biggest social networking site, but not even Mark Zuckerberg is immune to being hacked.” So can hacking be stopped? Well Arthur (2011) explains “hacking is possible because modern computer systems are so complex that there will always be a flaw to be exploited somewhere.” Likewise, it is not always the computer systems that make hacking possible; many hackers intrude profile of users down to their passwords. Beaver (2015) describes, “password hacking is one of the easiest and most common ways attackers obtain unauthorised network, computer, or application access. Therefore, passwords are one of the weakest links in the information of security chain.” It is almost certain that when
creating social media accounts or any other sites, it is advisable to use unique passwords. EC-Council (2009) explains “most users create passwords that they can easily remember, which can make passwords easier to crack.” This seems a common problem with many users; it is giving the hackers more of a chance in gaining unauthorised access to accounts. Also, it is advisable that users “use at least eight characters in each password and use at least one symbol, number, uppercase letter and lowercase letter.” (EC-Council, 2009)

Ultimately, Knittel and Sotto (2003) state, “Hackers use vast knowledge to better the computer industry. At the same time, however, there are those erase other people’s files, steal credit card numbers or vandalise web pages.” It can be understood that hackers can be used for legit purposes abiding by the law, this may be working for the government, although, this research focuses on the criminal hackers, whose intentions are to break the law and access personal information.

2.3.2 Identity Theft

One of the many risks that are correlated with sharing personal information on social media is potentially having identity stolen, which can be used cruelly against the user, this is known as identity theft. Hanel (2010) discusses “simply put, identity theft is the unlawful use of someone else’s personal information. This personal information can be used in many ways, including securing credit, making purchases, obtaining medical services, getting jobs, or evading criminal investigation.” Evidently, it is clear why identity theft can be damaging and painstaking to any victim as an attacker can implement many worrying issues and this can be problematic with the use of social media. Cifas (2016) explains that “the likes of Facebook, Twitter, LinkedIn and other online platforms are much more than just social media sites, they are now a hunting ground for identity thieves.” Furthermore, Cifas (2016) also confirms that “a 52% rise in young identity fraud victims in the UK. In 2015, 23,959 people aged 30 and under were victims of identity fraud. This is up from 15,766 in 2014, and is more than double the 11,000 victims in 2010.” Distinctly, identity theft is still an issue, as it has
risen by thousands within a few years, it seems that it will continue to rise within the next few years too. Astonishingly, stealing any information can result in disaster with “one fraudster enrolled himself on five different degree courses at the same university and had 17 fake identities, he collected student loans worth £65,595. It has also been identified that a further 1,000 applications as being suspicious and has alerted universities.” (Chapman, 2007)

2.3.4 Burglary

Surprisingly, burglary is one of the unknown risks when using social media. Bloxham (2011) states, “the majority of burglars use social media such as websites Facebook and Twitter to target their victims, with four out of the five criminals said social media websites were being used by burglars.” This is an interesting aspect as it demonstrates how valuable personal information is when posted on these networking sites. Nationwide (2016) remarkably explains “remember: a picture tells a thousand words, it’s not just holiday selfies that could help burglars make their way to your front door. A photo of a cat could help them to find out where you live.” A bold and true statement, but realistically true. Uploading and sharing photos can unravel a lot of information to criminals, where as for the user it is just seen as a picture. BBC-News (2017) recently revealed, “a woman has been charged with a spate of burglaries following a social media appeal. She is accused of 15 counts of burglary, three counts of fraud, one count of conspiracy to commit burglary and one count of theft by finding.” As of 2017, it is still apparent that this type of criminal activity is happening from the use of social media.
2.4 Other possible risks

Above are the only three of the many risks that can happen when using social media. There are other malicious risks that can be damaging and cause severe consequences to victims.

The other two possible risks that will also be explored are cyber bullying and phishing. These two are quite common when using social media sites and are a major concern.
2.4.1 Cyber Bullying

Cyber-bullying is a growing concern among social media users and can be used in many different ways. Hunter (2012) suggests, “Cyber-bullying is a type of bullying that use electronic media. People who cyber-bully can use email, text messages, and images accessed from a phone or computer. Web pages, blogs, chat rooms and social networking sites also carry bullying messages and pictures.”

Butterly (2013) illustrates that “Facebook, Ask.fm, Twitter were found to be the most likely sources of cyber-bullying.” The effects of cyber-bullying from networking sites can lead to many issues, which can affect users mentality. Coughlan (2016) states “there were hundred deaths by suicide among students in the previous year, with figures covering all the UK. It follows warnings last week that half of ambulance call-outs to a university were for self-harm or suicide attempts. Among the problems highlighted as a growing source of stress was the constant pressures of social media and the threat of cyber-bullying and victimisation.” It is undoubtedly that cyber-bullying is a current concern, which can leave students with long term issues from the result of using social media.

2.4.2 Phishing

Lininger and Vines (2005) explains, “Phishing is on course to overtake spam as the main Internet headache, with more sophisticated techniques surfacing everyday. In a standard phishing exploit, an unsuspecting victim receives can email that seems to come from a bank or other financial institution and which contains a link to a website where the user is asked to provide details.” This is a unique attack to gain information, however, phishers are now targeting social media sites and it is becoming a popular problem with users. Timm and Perez (2010) states “messages are often accompanied with some tone of urgency asking you to take action quickly in order that you don’t think about it – instead you just react.” When users read a message urging them to take action in regards to their social media accounts, they tend to panic and continue on with the process, although, this is when the problem begins. Moreover, Brunty, Miller and Helenek (2014)
discusses that "phishing can occur with any website available. This applies to social media sites as well. Many members list their full names, addresses, birthdays, educational background and current workplace, freely giving out personal information to anyone who wants it.” Users of social media sites, who display personal information that can be seen by anyone, are more at risk of being a victim.

2.5 Improving Security on Social Media

As risks of social media continue to affect its users, there are ways to improve this and protecting your accounts from unauthorised users and protecting your information. Wright (2015) states, “never use the same passwords for social media accounts. If you do it is a bit like having one master key, so if fraudsters find out what this is, they will be able to access all accounts. Choose passwords which are long, use a combination of lower and upper case letters, and include numbers.” Arguably, the discussion on passwords has been the main element in securing social media accounts and other accounts. Passwords are the key to access relevant information, and it advised to use different passwords at all times. This is to ensure that the accounts any individual have’s, will have less of a risk of being hacked, especially if the password include letters, numbers and special characters, as mentioned above, the longer the password the better, as it makes it more difficult for the hacker to crack, thus is why each password for each accounts should be different, it minimises the chances of criminals accessing these and taking what is confidential. Another factor that Facebook, Twitter and many other networking sites have included, is a tool where the user will get alerted when an unknown user have logged onto the account. This provides the social media user to be alerted when any suspicious activity is discovered and further action can be taken.

You can protect your identity, privacy and information by; setting basic security settings on any social media that is used, not posting sensitive information online, being wary about when you let others know your location or using software tools that anonymise you when online. (Gupta and Brooks, 2013)
Besides, many users of social media do not take advantage of privacy and security settings that are available for them, to make their accounts more secure and private. Facebook displays a lot of information, from phone numbers, date of births to where the user lives, all this information that is displayed is risky, however, a user can take this information off as it is optional but there are a variety of settings allowing to make accounts more secretive, locking photo’s that only certain friends or the user itself can access. By users altering settings they can benefit from it positively.

Completely, even when users change the privacy and security settings they are still at risk from other threats. Therefore, there is another method to improve the security of social media this is antivirus software. Koret and Bachaalany (2015) states, “antivirus software is a special security software that aims to give better protection than that offered by the underlying operating systems. In most cases, it is used as a preventative solution.” Software like these scan all content on laptops and now even mobile phone devices, erasing all risks. Nevertheless, companies who specialise in antivirus software have now aimed their security software to social media users where they suggest the strength of security on the chosen password, scan for scams; like phishing that is most common when using social media, malware and any other malicious activity that can be identified when scanned. This gives the users of social media more assurance and maybe worth in investing in this particular software to enhance the protection on the accounts.

2.6 Summary

Ultimately, this section has provided briefly the use of social media focusing on students within the age range of 16-24 and 18-24 year olds, it concentrates on different aspects within the use of social media. This follows, the advantages of using social media and how it can be beneficial when using the different platforms of it. With the disadvantages, it is understanding that there are many risk’s that are associated with social media; it outlines many of them, mainly focussing on Identity Theft, Hacking and Burglary. Although, it does include and
details other two possible threats that can happen and explains how they can be a threat to users. Lastly, it details the improvement on how users can enhance the security of their social media accounts. It provides the various ways in how this can be done, from passwords, changing the privacy settings to investing in antivirus software. The following chapters will investigate further in what approaches and methods is best used to conduct the rest of this study in finding out if students are aware of the possible threats and which site is the least secure and why?
CHAPTER THREE: METHODOLOGY

3.0 Introduction

Within Section of the study, the research methodology will outline and detail the methodological stages, justifying and reasoning why each method and approach has been chosen and how it will be used to accomplish the findings. The Method may be divided into sub-sections that deal with research design, participants, techniques and procedures and ethical considerations. (Saunders et al, 2016).

The information collected will be from primary and secondary data, which will deliver different viewpoints. Also, this can be delivered from implementing mixed methodology where both qualitative and quantitative data techniques are used, allowing to provide more in-depth information. In regards to primary data, the use of questionnaires and semi-structured interviews will be explored and discussed; students at Cardiff Metropolitan University will undertake these. Further explanation will be provided, reasoning why these methods were chosen.
3.1 Research Design

Saunders et al, (2016) illustrates “research design is the general plan on how the researcher will go about answering the research questions. The first methodological choice is whether to follow a quantitative, qualitative or mixed methods research design. Each research design will lead to potential ethical concerns and it will be important to consider these to minimise or overcome them.”

One way of differentiating quantitative research from qualitative research is to distinguish between numeric data (numbers) and non-numeric data (words, images, video-clips and other similar material). In this way, ‘quantitative’ is often used as a synonym for any data collection technique (questionnaire) or data analysis procedure (such as graphs or statistics) that generates or uses numerical data. (Saunders et al, 2016)

In contrast, ‘qualitative’ is often used as a synonym for any data collection technique (such as an interview) or data analysis procedure (such as categorising data) that generates or uses non-numeric data. (Saunders et al, 2016)

In deciding the, which methodological approach to use, the researcher has decided to use the combination of the both, and adopt the mixed methods approach. This will be discussed below in detail.

3.2 Samples

In selecting a sample to study, it should represent the full set of cases in a way that it is meaningful and which we can justify. (Becker, 1998)

The sample that the researcher has targeted for this research will be students at Cardiff Metropolitan University; the original plan was to target student’s ages 18-21 year old but giving the diverse age range within university, this has been increased to 18-24 year olds. This will allow gaining an increase in more students to take part, leading to more respondents.
Barnett (2002) argues, “that using sampling makes possible higher overall accuracy.” The researcher has decided to use a specific age range within this project, as it should provide a well-structured outcome, but also allowing to manage the set of results professionally and accurately. The targeted students will need to be the minimum age of 18 to participate, this allows reducing the issues surrounding the ethical documents, so it can be approved faster, allowing the primary research to be conducted quicker and also this is suitable as the minimum age for a university student is 18 years of age.
3.3 Mixed Methods

Mixed methods research is the branch of multiple methods research that combines the use of quantitative and qualitative data collection techniques and analytical procedures. (Saunders et al, 2016). This is where Creswell (2014) states “that the core assumption of this form of inquiry is that the combination of qualitative and quantitative approaches provides a more complete understanding of a research problem than either approach alone.”

From using these mixed methods, the both has their advantages and disadvantages that will be discussed below, however, the researcher has found it more approving in using this method as apposed to applying and using just the one, due to the reason, where the discussion from interviews are more defined and in-depth compared to questionnaires, where the discussion is more limited.

3.4 Questionnaires

The questionnaire is one of the most widely used data collection methods within the survey strategy. Because each person (respondent) is asked to respond to the same set of questions, it provides an efficient way of collecting responses. (Saunders et al, 2016). The researcher investigated the different methods to collect data, and came to the decision to include questionnaires within this research. To use this method, it is described that questionnaires therefore tend to be used for descriptive research, such as that undertaken using attitude and opinion questionnaires, enables to identify and describe the variability in different phenomena. (Saunders et al, 2016). When taking this into account, it is reminded that the researcher has to focus the questionnaire on the research topic. Furthermore, it entails that the questionnaire should allow forming the opinion and the view from students in regards to the security issues surrounding social media and the use of social media used. In total there were 14 questions in total, with 50 questionnaires were handed out and 40 were returned completed. The questionnaire is self completed by the respondents; however, they are
distributed and are accessed via an anonymous link, allowing in getting quicker responses.

Initially, it was planned that more interviews was going to be conducted and fewer questionnaires, however, the researcher have changed this to conducting more questionnaires and fewer interviews. This reasoning behind this change was that questionnaires would allow gathering more information quicker and faster and it can be distributed in many ways. The interviews will be discussed in detail below.

3.4.1 Questionnaire Design

The internal validity and reliability of the data that is collected and the response rate you achieve depends, to a large extent, on the design of the questions, structure of the questionnaire and the rigour of the pilot testing. (Saunders et al, 2016). It is evident that the design of the questionnaire can affect the information collected depending on how the structure and design is set out. Furthermore, Foddy (1994: 17) discusses “validity and reliability in terms of the questions and answers making sense. In particular, the question must be understood by the respondent in the way intended by the researcher and the answer given by the respondent must be understood by the researcher in the way intended by the respondent.” It is strongly suggested that not just the design of the questionnaire but the wording of it must be clear to read and analyse allowing the respondent to answer it correctly and for the researcher to understand the opinions given, this gives the research a more accurate and stable results.

The design and structure of the questionnaire was important when the researcher constructed it. It is formed of questions that the research believes are simple and can be understood easily, allowing the respondent to answer it with confidence. There are a small handful of questions, allowing the questionnaire to be completed easily, and make’s it more approachable as the respondents will
tend to complete it, given that it is formed on a small scale rather than pages and pages of questions. If the questionnaire was on a larger scale, the researcher felt that the respondents would get bored easily and either answer the questions untruthfully or not complete it at all. Some questions are structured differently, allowing the respondents to choose their answer in a variety of ways, this will minimise the boredom of answering and also decrease the risk of incomplete questionnaires.

3.4.2 Questionnaire Advantages

There are many advantages of using questionnaires to collect data. The main elements of the advantages that are going be discussed and what the researcher took into consideration are, respondents are not under pressure to respond immediately as is often the case in interviews, respondents have greater feelings of anonymity and thus are more comfortable in expressing their real feelings on even personal or sensitive topics and the questionnaire can be mailed, is likely to be inexpensive, can reach more people, and will cover a wide area. (Cargan, 2007)

The researcher believes that the elements discussed above, can have a significant effect on the questionnaire. It can be seen that by using questionnaires, there are benefits in using this type of method to gather information, it allows the respondent to take the questionnaire truthfully as it is anonymous and can be done in their own time.

3.4.3 Questionnaire Disadvantages

Surprisingly, with advantages there’s often disadvantages, it is often argued that with questionnaires it is limited to the written responses to the prearranged questions. This may result in more “I don’t know” answers and incomplete information. Another factor that is interesting is the lower response rate to questionnaires may also be due to some respondent’s inability to answer simple
questions. Thus, the usual questionnaire may be appropriate only for people with certain level of education. (Cargan, 2007)

When taking these into account, it is advised that the structure and wording of the questions asked, is kept so that is self-explanatory so it minimises the risk of incomplete responses and can be answered without confusion.
3.5 Semi-Structured Interviews

The use of interviews can help to gather valid and reliable data that are relevant to your research questions and objectives. Interviews can also be used to help refine ideas. These are often referred to as qualitative research interviews. In semi-structured interviews the researcher has a list of themes and some possible key questions to be covered. (Saunders et al, 2016). Furthermore, one of the main benefits in using semi-structured interviews is they have an overall structure and direction but allow a lot of flexibility to include unstructured questioning. (Hair, 2015) Moreover, semi-structured interviews, also provide the researcher with the opportunity to ‘probe’ answers, where the interviewees will explain, or build on, their responses. (Saunders et al, 2016) This can be beneficial as the interviewees expanding on their responses can encourage more information, leading to achieving a variation of views. Also, they may also lead the discussion into areas that the researcher had not previously considered but which are significant for the understanding of the researcher. (Saunders et al, 2016)

This will be interesting in regards to this topic area, as it will provide interviewees, other risks of social media to discuss that may be an important factor within this research.

The researcher has examined the different type of interview methods and has decided the best method to gather information from is semi-structured interviews.

3.5.1 Semi-Structured Interview Layout

In total there were four interviews, with all being a student from Cardiff Metropolitan University. As semi-structured interviews will be used, there is no strict structure to this method, allowing the researcher and interviewee having flexibility in discussing new and expanding on different topic areas. The topic area that'll be discussed mostly will be the issues surrounding the use of social
media and, as different interviewee's will have different opinions on this topic, the timing of the interview will also vary. The researcher has stated that each interview will last around 10-15 minutes each, allowing the plenty of time for interviewees and the research to ask questions and collect responses. As the interviews will be one-to-one, it should not take no more than the stated times given. As each interview will be different, some may finish earlier and some may finish later than the time's provided. This may be because each participant will approach and answer the questions differently; some may become uninterested quickly, which may affect the response given. The researcher has took these possible problems into consideration, and have discussed that the interview should be no longer than 20 minutes maximum and have ensured the participants will be anonymous throughout this research.

3.6 Ethics

Before any primary or secondary research can be taken, the researcher had to put forward an ethical document to be approved. This is where the researcher had to discuss what research and samples etc. will be undertaken during the study.

This is confirmed as, Saunders et al, (2016) states, “many students want to start their research as soon as they have identified a topic area, forgetting that access and ethics are critical aspects for the success of any research project.” This is an important part of the research, as it is required to detail the required approaches the research is going to be used and how they are going to access the information, this is to ensure that no ethical concerns or problems will occur during the research of the study. It is later informed that ethical concerns are greatest where research involves human participation, irrespective of whether the research is conducted person-to-person. (Saunders et al, 2016). In order for the ethics to be approved by the Research Ethics Committee, there are additional documents needed depending on the methods chosen. As this study is using a mixed methods approach, consisting of questionnaires and semi-
structured interview, it was required to include the supporting documentation, which are, participant information sheet and participant consent sheet. These may be given or sent to intended participants or respondents. It should include information about the nature of the research, the requirements and implications of taking part, participant's rights, how their data will be analysed, reported and stored and whom to contact in the case of concerns. (Saunders et al, 2016) The researcher had to ensure, that these documents were sent with the main ethics document, including the information of this study.

One of the essential factors the researcher will need to assure the participants their anonymity and confidentiality, this will allow them to understand the type of consent they are being involved with. This leads onto the principles of Data Protection Act 1998 (data protection and management). Saunders et al (2016) discusses that original and anonymised data needs to be stored securely to protect these from unauthorised access. Security will take a number of forms. Paper copies of interview or observation notes, signed consent forms, structured observation forms, questionnaires, transcriptions and other documents that contain confidential or personal data need to be held in a restricted, secure and safe place. Data held on external hard disc drives, compact drives and other audio-recordings would also need to be held under the same conditions.

Throughout this research, it is constantly reminded that all participants will be kept as anonymous, allowing in keeping their identity as low as possible. Also, it is reminded that even after the research has come to a completion, their participation and information is still safe and will be kept safe, Saunders et al (2016) emphasises this as "the management of data illustrates how ethical concerns are likely to remain beyond the end of the research project in order to continue to maintain the confidentiality of the data that was collected, the anonymity of participants, their privacy and to ensure that harm is not caused to those who helped within the research."
3.7 Summary

Within this chapter, it has outlined the methods and approaches that were chosen for this research project and why these suited this research. It has detailed the use of qualitative and quantitative, the benefits of using these and the design/layout of questionnaires and semi-structured interviews has also been detailed.

It has also been discussed how the researcher has changed the sample of the primary data. Now there will be more questionnaires than interviews, whereas the researcher originally planned to conduct more interviews. However, due to the easy access and distribution of questionnaires, it seemed more realistic to change. Originally deductive research was going to be used, however, the researcher has decided to opt for inductive research, as this will allow to gather valuable data and analysing trends allowing to develop a theory.

It has been outlined who will be taking part within the research. Why these participants were chosen and how they helped significantly in the progression of the project. All the supported documentation will be at the appendices, including the main ethics document, the consent and individual participant sheets, questionnaires, interviews and transcripts of the interviews.

Overall, the researcher has defined the main elements of the methodology that will be used and why, also taking into consideration the ethical concerns.
CHAPTER FOUR: RESULTS

4.0 Introduction

This chapter will present the results from the primary research: questionnaires and interviews. Firstly it will briefly outline the questionnaire results, which will detail the questions asked, the possible answers and then answers collected which will be in percentages, the data highlighted explains which answer were selected the most from the respondents. Secondly, this will then follow on to the interview results, which was focussed on the topic of social media.

4.1 Questionnaire Results

This questionnaire was designed and completed through Cardiff Metropolitan University’s ‘Qualtrics Survey Software’ and was completed by 40 respondent’s, which all were completed through an anonymous link. The questionnaire was first given out on a trial basis at the beginning of March, after a few amendments, it was then made accessible and given out till the end of March to be completed. The questions asked are a mixture of the use of social media, mobile phones, how aware the students are of the dangers/risks associated with social media and change of passwords.

Table 4. Presents the questions asked, the possible answers, the percentage of each answer and the number of people who selected that answer. The information that is highlighted in red specifies the answer that was the most selected. However, one of the questions, there are two answers highlighted as they had the same number of respondents who selected them.

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
<th>Percentage</th>
<th>Number of People</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please select your age?</td>
<td>18</td>
<td>10%</td>
<td>4</td>
</tr>
<tr>
<td>Question</td>
<td>Response</td>
<td>Count</td>
<td>Percentage</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>Are you a social media user?</td>
<td>Yes</td>
<td>40</td>
<td>100%</td>
</tr>
<tr>
<td>Are you a frequent user of any of the sites listed?</td>
<td>Facebook</td>
<td>35</td>
<td>85%</td>
</tr>
<tr>
<td>Are you a frequent user of any of the sites listed?</td>
<td>Twitter</td>
<td>35</td>
<td>87.50%</td>
</tr>
<tr>
<td>Are you a frequent user of any of the sites listed?</td>
<td>Instagram</td>
<td>38</td>
<td>95.00%</td>
</tr>
<tr>
<td>Are you a frequent user of any of the sites listed?</td>
<td>Snapchat</td>
<td>39</td>
<td>97.50%</td>
</tr>
<tr>
<td>On what device do you mostly use social media?</td>
<td>Mobile</td>
<td>39</td>
<td>97.50%</td>
</tr>
<tr>
<td>Are you a frequent user of any of the sites listed?</td>
<td>Laptop</td>
<td>1</td>
<td>2.50%</td>
</tr>
<tr>
<td>How much time (roughly) would you say you spend on social media a day?</td>
<td>Less than a hour</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>How much time (roughly) would you say you spend on social media a day?</td>
<td>1-2 hours</td>
<td>8</td>
<td>20%</td>
</tr>
<tr>
<td>How much time (roughly) would you say you spend on social media a day?</td>
<td>2-3 hours</td>
<td>11</td>
<td>27.50%</td>
</tr>
<tr>
<td>How much time (roughly) would you say you spend on social media a day?</td>
<td>3-4 hours</td>
<td>10</td>
<td>25%</td>
</tr>
<tr>
<td>How much time (roughly) would you say you spend on social media a day?</td>
<td>More than 4 hours</td>
<td>11</td>
<td>27.50%</td>
</tr>
<tr>
<td>How many hours do you spend on your mobile phone?</td>
<td>0-2 hours a day</td>
<td>4</td>
<td>10%</td>
</tr>
<tr>
<td>How many hours do you spend on your mobile phone?</td>
<td>2-4 hours a day</td>
<td>9</td>
<td>22.50%</td>
</tr>
<tr>
<td>How many hours do you spend on your mobile phone?</td>
<td>4-6 hours a day</td>
<td>18</td>
<td>45%</td>
</tr>
<tr>
<td>How many hours do you spend on your mobile phone?</td>
<td>6+ hours a day</td>
<td>9</td>
<td>22.50%</td>
</tr>
<tr>
<td>Do you check your social media accounts when you wake up in the morning?</td>
<td>Yes</td>
<td>33</td>
<td>82.50%</td>
</tr>
<tr>
<td>Do you check your social media accounts when you wake up in the morning?</td>
<td>Sometimes</td>
<td>6</td>
<td>15%</td>
</tr>
<tr>
<td>Do you check your social media accounts when you wake up in the morning?</td>
<td>No</td>
<td>1</td>
<td>2.50%</td>
</tr>
<tr>
<td>Do you see any problems in putting any personal information on social media?</td>
<td>Yes</td>
<td>39</td>
<td>97.50%</td>
</tr>
<tr>
<td>Do you see any problems in putting any personal information on social media?</td>
<td>No</td>
<td>1</td>
<td>2.50%</td>
</tr>
<tr>
<td>Out of Facebook, Twitter and Instagram, which do you think is the least secure?</td>
<td>Facebook</td>
<td>22</td>
<td>56.41%</td>
</tr>
<tr>
<td>Out of Facebook, Twitter and Instagram, which do you think is the least secure?</td>
<td>Twitter</td>
<td>7</td>
<td>17.95%</td>
</tr>
<tr>
<td>Out of Facebook, Twitter and Instagram, which do you think is the least secure?</td>
<td>Instagram</td>
<td>10</td>
<td>25.64%</td>
</tr>
<tr>
<td>Do you agree or disagree that sharing/posting personal information</td>
<td>Agree</td>
<td>39</td>
<td>97.50%</td>
</tr>
<tr>
<td>Question</td>
<td>Agree</td>
<td>Disagree</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Effect of using social media on social media can cause Identity Theft, Hacking and Burglary?</td>
<td></td>
<td>2.50%</td>
<td></td>
</tr>
<tr>
<td>Have you ever been a victim of criminal activity such as Hacking, Identity Theft etc?</td>
<td>Yes</td>
<td>35%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>65%</td>
<td></td>
</tr>
<tr>
<td>Are you aware of the possible threats/dangers of social media?</td>
<td>Yes</td>
<td>85%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>15%</td>
<td></td>
</tr>
<tr>
<td>Have you ever changed any privacy settings on any of you social media accounts?</td>
<td>Yes</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>How often do you change your social media passwords?</td>
<td>Never</td>
<td>42.50%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every 1-5 months</td>
<td>15%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every 6 months</td>
<td>15%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every year</td>
<td>27.50%</td>
<td></td>
</tr>
</tbody>
</table>

**4.2 Semi Structured Interviews**

The semi-structured questions consisted of four questions and four students from Cardiff Metropolitan University were interviewed. The information from these interviews will allow the researcher to collect and analyse it, which will be discussed in the Discussions chapter. Each interview was recorded and lasted around 10-15 minutes as planned; these will be transcribed later and will be later discussed that will help in finding any patterns or trends. The researcher will be discussing the main trends that were collected just from the interviews; the full interview's that are transcribed can be viewed in the appendix F.

The first trend that can be seen is from question 1, where all four separately was asked what and how many social media accounts do they use.

Student 1: “I have four social media accounts, which are Facebook, Twitter, Instagram and Snapchat.”
Student 2: "I use four social media accounts; Facebook, Instagram, Snapchat and Twitter.”

Student 3: “I have and use Facebook, Twitter, Instagram and Snapchat. However the most site I use are Twitter and Snapchat.”

Student 4: “I use and have four social media accounts, these are Facebook, Instagram, Snapchat and Twitter. I mostly use all of these platforms of social media for different reasons. Although, Twitter, Instagram and Snapchat I use all the time.”

Surprisingly, all four students have and uses the same social media accounts: Facebook, Twitter, Instagram and Snapchat. The researcher was intrigued and then followed on with another question in why they use these sites and not other ones. Again there was a similarity in their responses.

Student 1: “I have had a Facebook account since 2009, at that time and still to this day Facebook was the trend in everyone I knew had an account. With Twitter and Instagram, I joined a few years later, maybe around 2013. Again, when these platforms were introduced, it was the new trend in regards to social media and they provided something different compared to Facebook. In regards to Twitter, Instagram and Snapchat, they are popularly used, so this is why I only have an account with these and not got an account with others.”

Student 2: I think that these four social media sites (Facebook, Twitter, Instagram and Snapchat) are the most popular, especially where I am from, nearly everyone uses these sites. I mostly use Twitter and Snapchat, however, in regards to other social media sites, I don’t know many people who I know that uses them, so therefore it don’t motivate me in creating account with other networking sites like Flickr etc.”

Student 3: “Well I remember joining Facebook as everyone at the time had joined and it was a trend to have a Facebook account. This was the same for the rest (Twitter, Instagram and Snapchat); however, I don’t use Instagram as much as I used to. In regards to other social media sites like Tumblr and Flickr, they are not so popular within my area, so it does not appeal to me in creating account.”
Student 4: “These four sites are popularly used by everyone, so at the times they were new, I had to create an account, and till this today they are all still popular. I know there are other social media sites, but they are not used as much as these, so I wouldn’t create an account for any other site because no one I know will be using them.”

Interestingly, there were different responses in relation to question 2; which was what kind of personal data is displayed on the social media accounts.

Student 1: “The social media site where most of my personal information is displayed on is Facebook. It displays my relationship status, date of birth, the area where I live, my current education in where I study and my previous school.”

Student 2: “Facebook is where most of my personal information is displayed, followed by twitter. Facebook, I have the current workplace in where I work, current and previous education, date of birth and mobile phone number.”

Student 3: “I don’t have much personal information shared on my social media accounts. The only personal information that is displayed is on my Facebook account which is my date of birth and that’s it.”

Student 4: “Facebook is the social media account where most of my personal information is displayed, these include; my phone number, date of birth, education, where I live and relationship status.”

So, with the third question, they were asked what risks could be caused through sharing personal data.

Student 1: “Honestly, when I first had my social media accounts, I didn’t think of the risks. However, I do believe there are risks, such as hacking and cyber-bullying that are associated with using these sites.”
- “Yes, I have changed settings on my Facebook account. This is due to when I first had Facebook I did receive messages from people who I didn’t know.”

Student 2: “I think there are risks and security issues that can be caused by sharing data on social media. The risks that I think are caused are hacking and identity theft. Reason why is because I know of people who have experienced these issues.”
- “No I haven’t changed any settings, but I think I will if I experienced any problems.”

Student 3: “I think there are many risks, these include; hacking, burglary and cyber-bullying. Not many people will relate that sharing personal data and images on social media can cause burglaries.”
- “I have changed my settings to make my accounts more secure, my Facebook, Instagram and Twitter is private, which means only people I know can access and see my information that I post.”

Student 4: “There’s always risks and I have a few in mind that can be caused from sharing personal information. The one risk that keeps coming up in relation to the security issues of social media is hacking. I have heard and know people who have been a victim of hacking.
- “Yes I have changed the settings on one of my accounts, Facebook.”

Finally with the final and fourth question it was asked in their own opinion what is the biggest risk that can be caused by sharing personal data and why.

Student 1: “I think that the biggest risk and security issue that can be caused from social media is hacking and cyber-bullying. Even though hacking is a major threat, I believe that cyber-bullying is much more severe, there are many forms that this risk can be done and can become dangerous.”
- “Yes, I am aware of the information that can be accessed, but I believe this information will not lead to anything major like hacking.”
Student 2: "I think the biggest risk that can be caused by sharing personal data is definitely hacking. The reason being is that in order to access the accounts, they must of known the password, this can lead to potentially other accounts being accessed and may lead to unauthorised access to bank accounts."

- "Yes I am aware of the information that can be accessed, I may change the settings to minimise the amount of information that can be accessed."

Student 3: "Personally, the biggest risk that can be caused from sharing personal information is hacking and burglaries. These two cause different implications and can lead to major consequences. Hacking can happen to many accounts, the amount of personal data that is stored on different sites, once hackers access these, a lot of data can be released. In contrast to burglaries, images are powerful, and burglars will depend on these and posts in targeting victims.

Student 4: "Hacking I see as one of the biggest risks and would be concerned if it happened to me. Hackers have the ability to access your account without permission and can easily take information."

4.3 Summary

This chapter has acknowledged the full results from the questionnaire and the key trends that are briefly identified from the interview results. When analysing the results from the interviews, there were some similarities themes in where the four students had accounts with Facebook, Twitter, Instagram and Snapchat, with the reason being that these are the most popularly used networking sites. When they were asked about not having an account with other social media sites, similarly, their response was that the people who they know do not have any other social media accounts, so it does not appeal to them in signing up to a new one. In regards to question 3, there were similar responses when asked about the possible risks that may be caused, all four respondents mentioned hacking, however, other risks were mentioned such as identity theft, burglary and cyber-bullying. This followed on with changing settings on their accounts; they are
stated that they have not changed any settings on any of their social media accounts. Finally, with the last question, they all mentioned that hacking is or is one of the biggest risks associated with sharing personal data, with cyber-bullying and burglary was mentioned once. These results have briefly detailed the similarities from the interviews.
CHAPTER FIVE: DISCUSSION

5.0 Introduction

This chapter will include the overall discussion of information collected from the qualitative and quantitative primary research and the secondary research: the relevant literature that has been discussed. The findings from the questionnaire will be discussed and then the semi-structure interviews will be included if it is relevant and can support the statement. This will then deliver an explanation of the results gathered and comparisons will be detailed, providing the key themes that can be identified.

5.1 Analysis and Discussion

Figure 5.1 Total Number of Respondents Per Age

From Figure 5.1, it details the age range of 18-24, with the number of respondents. It can be seen that majority of age respondents were 20 year olds with 12 participants, closely followed by 21 year olds with 10 participants.
Above, Figure 5.2 shows it can be seen that all participants is a member of social media, with 40 (100%). This may demonstrate that social media is mostly commonly used between 18-24 year olds. In addition this can be supported by the relevant literature in which Christopher (2015) states, “The use of social media is most common among 18-24 year olds.” These age groups influence the use of social media and are dominating the lives of these individuals in which are used by a variety of sites.

**Figure 5.3. Percentage of Respondents Who uses What Type of Social Media**
From Figure 5.3 – Surprisingly the majority of respondents are a user of Snapchat with 97.5%; Instagram closely follows with 95%, then Twitter with 87.5% and shockingly Facebook, with 85%. This may indicate that many do not trust Facebook. Snapchat may be the most popular as it is a different compared to the others, there are a couple of differences that make this program unique and one of the most interesting social media platforms in use today like using photos and videos to communicate with other people. (Scholl, 2016)

Student 1: “I have four social media accounts, which are Facebook, Twitter, Instagram and Snapchat.”
Student 2: “I use four social media accounts; Facebook, Instagram, Snapchat and Twitter.”
Student 3: “I have and use Facebook, Twitter, Instagram and Snapchat. However the most site I use are Twitter and Snapchat.”
Student 4: “I use and have four social media accounts, these are Facebook, Instagram, Snapchat and Twitter.”

These results from the questionnaire and interviews identify that Facebook, Twitter, Instagram and Snapchat are the most popularly used social media sites, this may indicate that these sites will still continue to be popular with young users, especially those aged 18-24.
Above, Figure 5.4 shows it is evident that mobile devices is the most popular used device for social media with 97.5% declaring that they use it compared to 2.5% who used a laptop. It is clear that the use of smartphones is dominating the lives of individuals, Ofcom.org (2015) can support this as they explain, “Smartphones has continued to increase – they are now the most widely-owned internet-enabled device”. Giving that smartphones are dominating the world of communication, it may be argued that the 97.5% from Figure 5.4 who uses this device will partly use it for social and networking purposes, giving the easiness of accessing social media accounts on smartphones. They provide users accessing it faster allowing communicating and sharing information quicker, compared to using a laptop/computer.
The above graph demonstrates the amount of hours that is roughly spent on social media a day from the respondents. What is interesting is that none of the participants spends less than an hour a day on social media. The majority spends 2-3 hours or more than 4 hours a day.

It can be discussed that from Figure 5.6, the majority of 18-24 year olds spend between 4-6 hours a day on their mobile phones. In contrast to the relevant literature, it was discovered that those aged 18-24 checked their mobile almost every 10 minutes (Yan, 2015). This is astonishing in how addictive a device can
be, it may suggest that, 18-24 years may check their phone every 10 minutes to check their social media accounts, giving that 97.5% of the respondents claimed they check their accounts on mobile devices.

The discussion from Figure 5.4 where most participants (97.5%) uses a mobile phone for social media purpose, Figure 5.5, where the majority spends 2-3 and more than 4 hours a day on social media and Figure 6 where 45% spends 4-6 hours a day on a mobile phone. All these can have a comparison in that all participants (18-24 year olds) have specified that they use a mobile for social media, spends around 4-6 hours a day on mobile phone and as much as more than 4 fours a day on social media. From this it can be understood the extent in how much social media and mobile phones are a part of the lives of the participants. From 40 students this pattern is fascinating; it can be debated that if the sample would have been on a larger scale, the pattern of results could be the same, giving that the majority of individuals use the same social media sites due to their popularity.

**Figure 5.7. Percentage of Respondents Who Check Social Media Accounts in Mornings**

Fascinatingly, 82.5% of participants expressed that they check their social media accounts in the mornings when they wake up, with only 15% expressing they do it sometimes, compared to a low 2.5% who explained they do not. In contrast to this area, it is claimed that during the day, 18-24 year olds are among the most enthusiastic of smartphone users. (Deloitte, 2016) From this, a key trend can be
discovered in the relationship between the use of social media and the use of smartphones. The participants clearly, have an interest in both, so it is understandably why social media is heavily used on mobile devices in the mornings but also throughout the day and night.

**Figure 5.8. Percentage of Respondents Who See’s that it is a Problem in Displaying Personal Information on Social Media**

Evidently, from Figure 5.8, it is clear that 97.5% of participants can understand that by sharing person information on these social media sites can cause problems, whereas 2.5% states that they do not see a problem with displaying personal information.

However, 97.5% of participants from the questionnaire have stated they do see a problem with displaying personal information on social media. Yet, from the interviews, 3 interviewees: students 1, 2 and 4 have explained below which information is displayed. With only student 3 explains that only their date of birth is displayed.
Student 1: “The social media site where most of my personal information is displayed on is Facebook. It displays my relationship status, date of birth, the area where I live, my current education in where I study and my previous school.”

Student 2: “Facebook is where most of my personal information is displayed, followed by twitter. Facebook, I have the current workplace in where I work, current and previous education, date of birth and mobile phone number.”

Student 3: “I don’t have much personal information shared on my social media accounts. The only personal information that is displayed is on my Facebook account which is my date of birth and that’s it.”

Student 4: “Facebook is the social media account where most of my personal information is displayed, these include; my phone number, date of birth, education, where I live and relationship status.”

Captivatingly, the majority can see a problem with displaying information on these sites, but the interviewee’s have a variety of personal information displayed on their social media accounts. So, it is confusing in how so many participants from the questionnaire is aware of the problems in displaying information on social media compared to the three participants who has personal information displayed on their accounts. One may argue that the difference in these views is from a personal perspective, in the way that some of the questionnaire participants have experienced a problem with social media, whereas the three interview participants who have a variety of personal information displayed have not experienced an issue with these sites. Consequently, student 3, whose social media accounts are private and have not got hardly any information displayed apart from the date of birth, thus may result in that this student have experienced a problem and resulting in why the private accounts and the very little information that is displayed.
It is clearly stated from the results above, that the participants view is that Facebook is the least secure social media site with 56.4% and Instagram being voted the most secure with 25.6%. However, this can down to the amount of information that is displayed on these sites.

From the interviews, all four interviewee's has stated that the social media site that displays the most personal information is Facebook. These can be seen below.

Student 1: “The social media site where most of my personal information is displayed on is Facebook.”

Student 2: “Facebook is where most of my personal information is displayed, followed by twitter. Facebook.”

Student 3: “I don’t have much personal information shared on my social media accounts. The only personal information that is displayed is on my Facebook account which is my date of birth and that’s it.”
Student 4: “Facebook is the social media account where most of my personal information is displayed, these include; my phone number, date of birth, education, where I live and relationship status.”

From the above discussion, Figure 5.9 states that 56.4% of participants believe that Facebook is the least secure social media site. This in contrast to the interviews has a similar comparison, where a trend can be identified as the majority of information is displayed on Facebook. This may result in why this site has been voted the least secure and maybe, if Facebook did not display as much personal information, then these results may differ.

**Figure 5.10. Percentage of Respondents who agreed and disagreed that Personal Information on Social Media can cause Hacking, Identity Theft and Burglary**

The majority (97.5%) of participants agreed that personal information on social media sites could cause hacking, identity theft and burglary. With only one 1 (2.5%) disagreed. This may result in that the participant’s (18-24 year olds) may know of people or may have been a victim of these issue’s resulting the high percentage who agreed.
The likes of Facebook, Twitter, LinkedIn and other online platforms are more than just social media sites; they are now a hunting ground for identity thieves. Also, there is a 52% rise in young identity fraud victims in the UK. (Cifas, 2016) Giving that social media platforms are becoming hunting grounds and identity fraud is on the increase, as the participants agree, this may demonstrate that users of social media may now be aware of the possible risks that are associated with using these sites.
From Figure 5.11, it is apparent that the majority (65%) of participants have not experienced or have not been a victim of any criminal activity in regards to hacking, identity theft etc. However, 35% of these claim they have been a victim. These may be done a variety of ways, conversely, password hacking is one of the easiest and most common ways attackers obtain unauthorised network, computer, or application access. Therefore, passwords are one of the weakest links in the information of security chain.” (Beaver, 2015)

Of the 35% that have been a victim, it may down to password hacking, it is one of the most popular cyber-crimes and the easiest way that hackers can access accounts, this may suggest passwords can be a problem for some, especially those with weak or use the same passwords for multiple accounts.
Additionally, when asked about the awareness of the possible threats/dangers of using social media, 85% of the participants stated they are aware of the dangers of using it, with only 15% stating they are not aware. With those who are not aware and sometimes those who aware of the risks, it is vital to know the use of blogs and social networking sites is an area of particular concern, as the security of such sites is often not well understood by users. Very often the default security settings allow everyone to see submitted information. (Gov.UK, 2011) The security of social media is a major concern, the security settings on all social media is a powerful section, this could protect so much information that a user displays, if users can understand the risks that are associated with using these sites, they may be persuaded to change their settings.

Furthermore, when comparing the results from the questionnaire to interviews, there does seem that 18-24 year olds are aware of the possible threats and dangers of social media. Below, displays the results from the interviews.
Student 1: “Honestly, when I first had my social media accounts, I didn’t think of the risks. However, I do believe there are risks, such as hacking and cyber-bullying that are associated with using these sites.”

Student 2: “I think there are risks and security issues that can be caused by sharing data on social media. The risks that I think are caused are hacking and identity theft. Reason why is because I know of people who have experienced these issues.”

Student 3: “I think there are many risks, these include; hacking, burglary, cyber-bullying and phishing. Not many people will relate that sharing personal data and images on social media can cause burglaries.”

Student 4: “There’s always risks and I have a few in mind that can be caused from sharing personal information. The risks that I think are in relation to the security issues of social media are hacking and phishing. I have heard and know people who have been a victim of hacking.”

From the above results, it can be illustrated that 18-24 year olds understand the awareness of the possible dangers from using social media. Figure 5.12, provides that 85% of these students are aware, comparing this to the replies from the interviews. The four students have provided different views on what kind of risks that can be opposed form using the sites. However, the main risks were hacking, cyber-bullying, burglary and phishing.
From Figure 5.13, it is apparent that 90% of the participants have changed their privacy settings on their social media accounts, with only 10% stating they have not. This may identify the reason why the majority (97.5%, Figure 5.11) stated that they agree that personal information can result in hacking and identity theft etc. If they are aware of the possible dangers, then it is more than likely users will change their account settings, making it more private and secure.

These results in comparison to those from the interviews are intriguing. From the four interviewed, only three; students 1, 3 and 4 have changed at least one setting on their social media accounts. Below provides the responses from interviews.

Student 1: “Yes, I have changed settings on my Facebook account. This is due to when I first had Facebook I did receive messages from people who I didn’t know.”
Student 2: “No I haven’t changed any settings, but I think I will if I experienced any problems.”

Student 3: “I have changed my settings to make my accounts more secure, my Facebook, Instagram and Twitter is private, which means only people I know can access and see my information that I post.”

Student 4: “Yes I have changed the settings on one of my accounts, Facebook.”

Ultimately, a pattern can be identified in that Students 1, 3 and 4 have changed their settings. However, these are all changed on Facebook. Student 1 explained that they were receiving messages from people who they did not know. So, why have they changed the settings solely and mostly on Facebook?

Remarkably, when analysing the discussion from Figure 9, 56.4% of participants believed that Facebook is the least secure social media site. So when comparing these results, both identifies the key theme, which is Facebook, it is where students have changed their settings and it has been voted the least secure site. Additionally, it seems that Facebook is appearing to be the most discussed about social media site in regards to the security and the change of settings, it could be argued that the same result may apply if the research was investigated on a larger scale, and those may imply that they results will be similar due to the popularity of the site, the amount of information that is shown and the lack of security.
From Figure 5.14, it is obvious that 42.5% have stated they have never changed their password on their social media accounts, with 27.5% claiming they change it every year, 15% changes it every 1-5 months and 15% changing it every 6 months. From this result it is overwhelming to confirm that the majority have never changed their social media passwords, it is illustrated above that password hacking is one of the easiest and most common ways to hack an account. Given those who have never changed their password every year, these will be more than likely to become victims of getting hacked or some other form of cyber-crime. Supportively, EC-Council (2009) explains “most users create passwords that they can easily remember, which can make passwords easier to crack.” So, if the users have used passwords that have a personal meaning, as in family name etc., and if these were used to set up accounts on social media, hackers will have a higher probability in accessing accounts faster and easier.
CHAPTER SIX: CONCLUSION

6.0 Introduction

This chapter will firstly detail and allow seeing if the objectives have been achieved throughout this study. The aim of this dissertation was to explore the risks that are associated with the use of social media sites and investigating how aware student's (18-24 year olds) are of these risks. Each objective will have an explanation below, detailing these and the aims has been achieved or not with supportive findings. Secondly, it will outline the main key themes that have been identified from chapter five: discussions, allowing summarising the overall the themes that have been produced.

6.1 Objectives Set

1. To discover the use of social media and why it has become so popular in today's society.

From the literature review it is evident that the in 2012 the UK was the second most prolific users of social media in Europe with almost 48% using social networking sites, such as Facebook and Twitter. Yet, the use of social media is most common among 18-24 year olds, with 91% of Internet users in this group owning a Facebook account. (Christopher, 2015) According to Ofcom.Org (2016) it is also apparent that 84% of 16-24 year olds visits any social media site or app more than once a day, statistics from this research can support this as similarly, Figure 5 shows that the majority of 18-24 year olds spends 2-3 hours a day and 4 or more hours a day on social media. This may result in how popular these networking sites really are and how they have become a part of many people’s lives. As social media users increase, so does the use of smartphones. It is clear that social media plays a huge part in many individual lives but so does smartphones, it is claimed that they are now the mostly widely-owned internet-
enabled device, with 18-24 year olds checking their mobile almost every 10 minutes. This compared to the 82.5% of questionnaire participants who expressed that they check their social media accounts in the mornings when they wake up, provides an insight in that social media will continue to grow and increase in number in regards to users. Also, it explains that the most users that are influenced and attracted to these sites are 18-24 year olds with 100% participants from the questionnaire state they are a social media member and user. However, with the change in the way we communicate, this may change and that these sites, may attract younger and even older users in time to come.

2. To explore the possible risks that can be occurred from using social media sites through relevant literature and primary research.

Many have claimed that as social media increases in users, so does the popularity. This will result in the number of risks will also increase. The possible risks that have been research was hacking, identity theft and burglary, with other possible risks being researched such as cyber-bullying and phishing. Harwood (2010) states, "unfortunately, spammers, hackers, phishers, and others see a medium that they may be to exploit by gaining confidential information." Hacking is one of the major and common risks associated with social media, with Cross (2013) stating that “can have far-reaching implications.” Everyone is prone to being hacked, as password hacking is one of the easiest and most common ways attackers obtain unauthorised access. (Beaver, 2015). However, from primary research, 42.5% have stated that they have never changed their passwords on their social media accounts. This makes them more vulnerable in becoming hacked.

From the interviews, all four interviewees mentioned hacking is one of the risks that can be caused from using social media. With identity theft, this risk is on the increase with 52% rise in young identity fraud victims in the UK. Many burglars use social media platforms to target their next victims, with four out five criminals said these criminals were using social media. From the primary research, 35% have been a victim of these crimes in regards to social media, with
97.5% agreed that hacking, identity theft and burglary can be caused from posting personal information on these sites. Furthermore, hacking, identity theft, burglary, phishing and cyber-bullying were all mentioned at least once, when asked about what risks could be caused from using social media.

It can be gathered from above that, many risks can be caused from using and posting personal information on these social media sites. The most common risks investigated and have been mentioned by students, were hacking, identity theft, burglary, cyber-bullying and phishing, with the majority agreeing that by posting personal information, these risks can occur.

3. To analyse how aware students are in regards to the risks, through primary research: questionnaire and semi-structured interviews and see which social media site is the least sure from a student’s perspective and why?

Figure 12 demonstrates that 85% of participants are aware of the possible dangers of social media, with 15% who are not aware. This in comparison with 90% who have changed their privacy settings on their accounts, may demonstrate that 18-24 year olds are aware of the possible risks, but do not fully trust these social media sites with protecting their information, hence why the majority have changed their settings. In comparison to the interviews, three of the four students have discussed that they have changed their settings but mostly on one social media site, Facebook. In contrast to one the questions, 56.4% selected that Facebook is the least secure social media site from a student’s perspective. This can be supported as the interviewees stated the following:

Student 1: “The social media site where most of my personal information is displayed on is Facebook.”
Student 2: “Facebook is where most of my personal information is displayed, followed by twitter. Facebook.”

Student 3: The only personal information that is displayed is on my Facebook account which is my date of birth and that’s it.”

Student 4: “Facebook is the social media account where most of my personal information is displayed, these include; my phone number, date of birth, education, where I live and relationship status.”

So arguably, from a student perspective, the majority are aware of the risks that can be caused from using social media; with the majority stating Facebook is the least secure purely because it displays the most information.

The overall conclusion provides the use of social media is increasing rapidly, although there are risks involved with students discussing and agreeing that hacking, identity theft and burglary and more can be caused from using these sites. However, in contrast to this, results show that students are aware of these possible risks with changing their privacy settings but not changing their passwords often.

6.2 Future Work

To further this study more, it would be interesting to investigate which social media site is the least secure and why from young users perspective and comparing this to older users. Arguably, it will be intriguing to gather statistical data and conduct interviews with multiple users, then comparing these to find any key themes, and to see if the both young and older users chose Facebook as the least secure or chose a different site and then compare the reasons why. The security of social media will always be an issue and finding out the least secure site, will be interesting, as new theories and knowledge will developed.
7.0 References


**Appendix A – Ethics Form**

When undertaking a research or enterprise project, Cardiff Met staff and students are obliged to complete this form in order that the ethics implications of that project may be considered. **If the project requires ethics approval from an external agency (e.g., NHS), you will not need to seek additional ethics approval from Cardiff Met. You should however complete Part One of this form and attach a copy of your ethics letter(s) of approval in order that your School has a record of the project. The document *Ethics application guidance notes* will help you complete this form. It is available from the Cardiff Met website. The School or Unit in which you are based may also have produced some guidance documents, please consult your supervisor or School Ethics Coordinator. Once you have completed the form, sign the declaration and forward to the appropriate person(s) in your School or Unit.**

**PLEASE NOTE:**

Participant recruitment or data collection MUST NOT commence until ethics approval has been obtained.

### PART ONE

<table>
<thead>
<tr>
<th>Name of applicant:</th>
<th>Benjamin Donoghue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor (if student project):</td>
<td>Stuart McNeil</td>
</tr>
<tr>
<td>School / Unit:</td>
<td>Cardiff School of Management</td>
</tr>
<tr>
<td>Student number (if applicable):</td>
<td>ST20071147</td>
</tr>
<tr>
<td>Programme enrolled on (if applicable):</td>
<td>BSc (Hons) Business Information Systems</td>
</tr>
<tr>
<td>Project Title:</td>
<td>Risks; Hacking, Identity theft, burglaries that are associated with Cardiff Met students (aged 18-2) with sharing personal data through social media applications; Facebook, Twitter and Instagram</td>
</tr>
<tr>
<td>Expected start date of data collection:</td>
<td>14/12/2016</td>
</tr>
<tr>
<td>Approximate duration of data collection:</td>
<td>1 Month</td>
</tr>
<tr>
<td>Funding Body (if applicable):</td>
<td>N/A</td>
</tr>
<tr>
<td>Other researcher(s) working on the project:</td>
<td>N/A</td>
</tr>
<tr>
<td>Will the study involve NHS patients or staff?</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve human samples and/or human cell lines?</td>
<td>No</td>
</tr>
<tr>
<td>Does your project fall entirely within one of the following categories:</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Paper based, involving only documents in the public domain</td>
<td>No</td>
</tr>
<tr>
<td>Laboratory based, not involving human participants or human samples</td>
<td>No</td>
</tr>
<tr>
<td>Practice based not involving human participants (eg curatorial, practice audit)</td>
<td>No</td>
</tr>
<tr>
<td>Compulsory projects in professional practice (eg Initial Teacher Education)</td>
<td>No</td>
</tr>
<tr>
<td>A project for which external approval has been obtained (e.g., NHS)</td>
<td>No</td>
</tr>
</tbody>
</table>

If you have answered YES to any of these questions, expand on your answer in the non-technical summary. No further information regarding your project is required.
If you have answered NO to all of these questions, you must complete Part 2 of this form.

In no more than 150 words, give a non-technical summary of the project.

In this project, its aim is to find all the possible risks that are associated with students sharing personal information through the use of social media applications such as Facebook, Twitter and Instagram. It will include primary and secondary research, including qualitative methods, utilising: questionnaires and semi-structured interviews. Patton (2014) stated, “*qualitative inquiry is fundamentally about capturing, appreciating and making sense of diverse perspectives.*” This should allow to get a range of diverse data. With secondary data that will be gathered from journals, articles and passed research papers.

**DECLARATION:**
I confirm that this project conforms with the Cardiff Met Research Governance Framework.

I confirm that I will abide by the Cardiff Met requirements regarding confidentiality and anonymity when conducting this project.

**STUDENTS:** I confirm that I will not disclose any information about this project without the prior approval of my supervisor.

| Signature of the applicant: | Date: 03/12/2016 |
| B. Donoghue | |

**FOR STUDENT PROJECTS ONLY**

| Name of supervisor: | Date: 11/12/2016 |
| Stuart McNeil | |

| Signature of supervisor: |
| Stuart McNeil |

**Research Ethics Committee use only**

| Decision reached: |
| Project approved x |
| Project approved in principle |
| Decision deferred |
| Project not approved |
| Project rejected |

| Project reference number: TBA |

| Name: Dr Hilary Berger | Date: 11/12/2016 |
| Dr Hilary Berger |

| Details of any conditions upon which approval is dependant: |
| None |
### PART TWO

#### A RESEARCH DESIGN

<table>
<thead>
<tr>
<th>A1 Will you be using an approved protocol in your project?</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 If yes, please state the name and code of the approved protocol to be used</td>
<td>No</td>
</tr>
<tr>
<td>A3 Describe the research design to be used in your project</td>
<td>Within this project primary research will be conducted in which the selected methods will be discussed below. An interpretative research philosophy will be adopted using deductive research strategy for collecting data, which is explained below. Questionnaires will be used on the (20/12/16) as an explorative research: this method is the quickest and easiest approach to collect data from students. The data that will be collected is the attitudes, opinions and behaviour data variables that then can be converted statistically. As Robson (2011) explains “they work best with standardised questions that you can be confident will be interpreted the same way by all respondents”. Semi-structured Interviews will be conducted at Cardiff Met on (17/01/16): this will give another insight of the attitudes and opinions from students. Samples – a sampling technique; convenience that will allow to target students (18 – 21 year olds) within Cardiff area, as Becker (1998) explains, “selecting a sample to study, it should represent the full set of cases in a way that is meaningful and which we can justify”. The size of participants will be 10 students for the questionnaire and 20 students for the interviews. Students will be recruited in Cardiff Metropolitan University. The participation for questionnaires should take no longer than 10 minutes and for the interviews it’ll be around 15-20 minutes. Their confidentiality will be protected as they will not put any personal identity information on the questionnaire, it will be anonymous. Excel as a tool will be used to produce statistical information through the use of graphs, tables and charts and also be the use of thematic technique to analyse data.</td>
</tr>
<tr>
<td>A4 Will the project involve deceptive or covert research?</td>
<td>No</td>
</tr>
<tr>
<td>A5 If yes, give a rationale for the use of deceptive or covert research</td>
<td>N/A</td>
</tr>
<tr>
<td>A6 Will the project have security sensitive implications?</td>
<td>No</td>
</tr>
<tr>
<td>A7 If yes, please explain what they are and the measures that are proposed to address them</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### B PREVIOUS EXPERIENCE

B1 What previous experience of research involving human participants relevant

---

1 An Approved Protocol is one which has been approved by Cardiff Met to be used under supervision of designated members of staff; a list of approved protocols can be found on the Cardiff Met website here
to this project do you have?

In second year of university as part of a particular module 'E-Business' I had to conduct an interview with my chosen company to gather data about their business.

<table>
<thead>
<tr>
<th>B2 Student project only</th>
</tr>
</thead>
<tbody>
<tr>
<td>What previous experience of research involving human participants relevant to this project does your supervisor have?</td>
</tr>
<tr>
<td>16 years of experience.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C POTENTIAL RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1 What potential risks do you foresee?</td>
</tr>
<tr>
<td>1. Not getting the questionnaires done in time.</td>
</tr>
<tr>
<td>2. Arranging interviews with students.</td>
</tr>
<tr>
<td>C2 How will you deal with the potential risks?</td>
</tr>
<tr>
<td>1. Time management will be key and by using a timely planned schedule should allow in getting the questionnaires done in time.</td>
</tr>
<tr>
<td>2. Interviews will be arranged in advanced, which will allow students to ensure that they have free time on the arranged date and time.</td>
</tr>
</tbody>
</table>

When submitting your application you **MUST** attach a copy of the following:

- All information sheets
- Consent/assent form(s)

An exemplar information sheet and participant consent form are available from the Research section of the Cardiff Met website.
PARTICIPANT INFORMATION SHEET

**Risks associated with students with sharing personal data through social media.**

**Cardiff Metropolitan University Protocol Number:**

**Project summary**
The purpose of this research is to determine the risks that there is with students sharing personal information through social media. Your participation will allow gathering a range of data, which will be included within a research study being undertaken at Cardiff Metropolitan University.

**Why have you been asked to participate?**
As the study is focused on students (aged 18-21) you have been asked to participate purely because you fit the profile of the target area that is being studied. You will be asked before any interview of course if you do use any social media first as this study is focused on that area. Your participation is entirely voluntary and you may withdraw at any time.

**Project risks**
The research involves an interview with a only a number of questions being asked. However, if you do feel any questions are inappropriate then you can stop at any time and withdraw.

**How we protect your privacy**
All the information you provide will be held in confidence and certainty. The only personal information that will be on the form will be your signature and this will be kept in a secure location by the research team. All consent forms will be kept for certain number of years after the study but will be kept securely.

YOU WILL BE OFFERED A COPY OF THIS INFORMATION SHEET TO KEEP

If you require any further information about this project then please contact:
Ben Donoghue, Cardiff Metropolitan University
Cardiff Metropolitan University email: st20071147@cardiffmet.ac.uk
Supervisors email: SMcNeil@cardiffmet.ac.uk

Cardiff Metropolitan University
Ethics Committee
### PARTICIPANT CONSENT FORM

Cardiff Metropolitan University Ethics Reference Number: **2016D0259**

**Participant name or Study ID Number:**

**Title of Project:** Risks associated with students with sharing personal data through social media

**Name of Researcher:** Ben Donoghue

<table>
<thead>
<tr>
<th>Participant to complete this section:</th>
<th>Please initial each box.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered reasonably.</td>
<td></td>
</tr>
<tr>
<td>2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.</td>
<td></td>
</tr>
<tr>
<td>3. I agree to take part in the above study.</td>
<td></td>
</tr>
<tr>
<td>4. I agree to the use of anonymised quotes in publications.</td>
<td></td>
</tr>
<tr>
<td>5. I agree to the interview being recorded.</td>
<td></td>
</tr>
</tbody>
</table>

**Signature of Participant**

_________________________________________   ___________________

**Date**

**Name of person taking consent**

_________________________________________   ___________________

**Signature of person taking consent**

_________________________________________
### Appendix D - Semi Structured Interviews

#### Semi-Structured Interview

<table>
<thead>
<tr>
<th>Order of semi structured Interview</th>
<th>Discussed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) What and how many social media accounts do you use?</td>
<td></td>
</tr>
<tr>
<td>2) What kind of personal data that is shared/that are displayed on these social media accounts?</td>
<td></td>
</tr>
<tr>
<td>3) What kind of risks do you think can be caused by sharing personal data through social media and how?</td>
<td></td>
</tr>
<tr>
<td>4) In your opinion what is the biggest risk that can be caused by sharing personal data through the use of social media and why?</td>
<td></td>
</tr>
</tbody>
</table>
# Appendix E – Questionnaire

<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Please select your age</td>
</tr>
<tr>
<td>18</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
</tr>
<tr>
<td>24+</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q2</th>
<th>Are you a Social Media user?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q3</th>
<th>Are you a frequent user of any of these sites listed below? (multiple choice)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
</tr>
<tr>
<td>Instagram</td>
<td></td>
</tr>
<tr>
<td>Snapchat</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q4</th>
<th>On what device do you mostly use Social Media on?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td>Laptops</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q5</th>
<th>How much time (roughly) would you say you spend on Social Media a day?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than an hour</td>
<td></td>
</tr>
<tr>
<td>1-2 hours</td>
<td></td>
</tr>
<tr>
<td>2-3 hours</td>
<td></td>
</tr>
<tr>
<td>3-4 hours</td>
<td></td>
</tr>
<tr>
<td>More than 4 hours</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q6</th>
<th>How many hours do you spend on your mobile phone?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-2 hours a day</td>
<td></td>
</tr>
<tr>
<td>2-4 hours day</td>
<td></td>
</tr>
<tr>
<td>4-6 hours a day</td>
<td></td>
</tr>
<tr>
<td>6+ hours a day</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q7</th>
<th>Do you check your Social Media accounts when you wake up in the morning?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sometimes</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q8</th>
<th>Do you see any problems in putting any personal information on Social Media?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Q8: Place the following Social Media sites (Facebook, Twitter and Instagram) in order of which you think is the least secure of keeping/displaying your information? (Top being the least secure and bottom being the most)

- Facebook
- Twitter
- Instagram

Q9: Do you agree or disagree that sharing/posting personal information on Social Media can cause Hacking, Identity Theft and Burglary?
- Agree
- Disagree

Q10: Have you been a victim of any criminal activity such as Hacking, Identity theft etc?
- Yes
- No

Q11: Are you aware of the possible threats/dangers of Social Media?
- Yes
- No

Q12: Have you ever changed any privacy settings on any of your Social Media accounts, to make your account more secure and private?
- Yes
- No

Q13: How often do you change the passwords of your Social Media accounts?
- Never
- Every 1-5 months
- Every 6 months
- Every year
Appendix F – Interview Transcripts
Q1: I want to make sure under accurate, which are accurate. Accurate, inaccurate.

Q2: So, why do you need someone at the error?

Q3: I have some pieces of social media accounts, which are more popular, essentially more. I can learn about the accounts, more users, and so on. I can learn about it. Learning is necessary, we found.

Q4: Someone is more about my personal information, I think. Followed by someone, I think. Inaccurate, but inaccurate. I want to see the personal information. I want to see the personal information of one.

Q5: I think sure we have not privacy and need is to have my privacy secured and we need more. The more I found we need more. Privacy is learning about personal. I think. It's different. I have more people, more how experienced under it. More people at the more they found. In the learning it can find more.

Q6: Have you changed my personal setting? Now it's important. I think; I don't know. I repaired my preferences.
75