Title: Cyberharassment and cyberbullying: individual and institutional perspectives

Name: Georgiana Alexandra Dobocan

CYBERHARASSMENT AND CYBERBULLYING; INDIVIDUAL AND INSTITUTIONAL PERSPECTIVES

BY

GEORGIANA ALEXANDRA DOBOCAN

A thesis submitted to the University of Bedfordshire, in partial fulfilment of the requirements for the degree of MSc by Research.

OCTOBER 2013

To my sister

For the fine lady you have become.

For the daily Batman jokes and your support.

ACKNOWLEDGEMENTS

Thank you **God** for giving me the strength, ingenuity, and the most fantastic people I have ever met, to guide me though this past year.

First and foremost, thank you **Prof. Maple** and **Dr. Short** for offering me the opportunity of undertaking this research within the National Centre for Cyberstalking Research which you co-direct. I will be forever grateful for this.

Thank you **Dr. Emma Short** for going out of your way to pass your knowledge onto me. Thank you for being more than just a traditional supervisor, for being a role model and an inspiring woman.

Prof. Carsten Maple, thank you for answering your phone whenever I called and encouraging me in my moments of doubt. Thank you for calmingly managing all of my panic attacks.

Even though you cannot read English, thank you **Mother** for the long Skype sessions in which you told me off for not taking my vitamins. **Father,** thank you for taking everything so lightly and always make me laugh. You two are the best parents anyone can ask for.

Rita Mascia, you changed my life. Thank you for 'adopting' me and teaching me how to manage my finances so I can buy more pairs of shoes.

For the time when I could not number my thesis pages and for the all of the previous times you were there for me, **Dr. Antony Brown**, thank you. I shall not forget that.

For not telling anyone I once cried, and for all of the times you got me out of the office in the evening, to unwind and change the scenery, thank you **Dr. Kristoffer Getchell.**

I don't have that many friends but you folks, did prove yourselves and since I overused the candy trick, I would like to thank you once more **Irina, Valentin, Adrian, Ema, Anca, (Lidia).**

I could not have conducted my research focus groups without your help **Gavin Steward**. Thank you. Also, I appreciate you taking time to discuss all of those interesting research angles whenever we met.

University of Bedfordshire has been my home not just for the past year but for the past four years and most of the staff members have been my friends and family. **Thank you all**. **Helen Green**, you made my research work fun, by adding the sporadic shopping sessions. Thank you for proofreading this piece.

ABSTRACT

Research on finding a relationship between institutional policy and the proliferation of cyberstalking, cyberharassment and cyberbullying in young adults, is limited. A National Institute of Justice (1998) study on a 4,446 USA student sample reveals that stalking on university campuses has a different profile than stalking nationally because of the nature of their mate-seeking age, proximity of the perpetrator to its victim and the facile way of accessing personal information. For this study, data from an undergraduate sample was gathered. Data suggests that online communication is ambiguous and there is a need for online norms, to which young people can adhere. Participants were generally not aware that the university had a policy on acceptable use of network. Moreover, participants were sensitive to being harassed and while being aware of how they were affected by the online behaviour of others, there was less certainty of the effects of their own behaviour.

CONTENTS OF FIGURES

1. INTRODUCTION

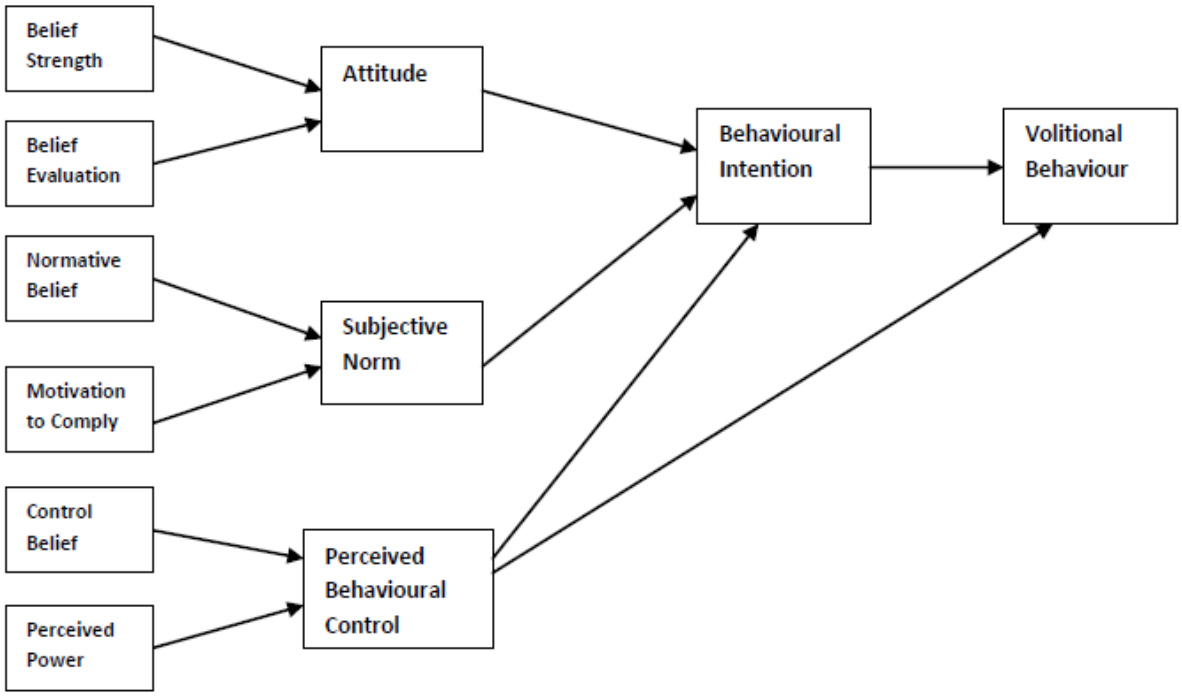
Even though stalking has been a known phenomenon for more than a century, it has only evolved into a real social issue within the last decades (Mullen, Pathe & Purcell, 2001). Continued technological advances as well as the internet revolution have made it more difficult for one to maintain anonymity. The psychiatric literature defines stalking as a course of conduct by which one person repeatedly inflicts on another, unwanted intrusion to such an extent that the recipient fears for his or her safety (Mullen, Pathe & Purcell, 2004). Stalking or causing distress to someone, by electronic means, has been referred to as cyberstalking. Cyberstalking can be defined as "threatening behaviour or unwanted advances directed at another using the internet and other forms of online and computer communications" (National Centre for Victims of Crime, 2003). In both cases of stalking and cyberstalking victims `reactions are of negative nature and include fear, depression, stress, anxiety, lowered self-esteem and loss of trust in other people (Mechanic et al., 2000). In 2007, Lenhart et al. (2008) found that 85% of teenagers (12-17) engage in some form of electronic personal communication at least occasionally (sending e-mails or instant messages, text messaging or posting comments on social networking sites). Even though the prevalence and incidence of cyberstalking remain undetermined, anecdotal reports suggest that the phenomenon appears to be expanding at a rapid pace, especially amongst the youths (digital natives)(Alexey,Burgees & Baker, 2005).

2. Related Work

2.1. Understanding Behaviour

2.1.1. Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) has received considerable credit in (social) psychology literature as it brings forward an integrated model of behaviour and it is one of the most widely researched models. Ajzen and Fishbein's (1980) theory of reasoned action (TRA) and TPB were developed to explain how persuasive forces and motivational beliefs drive intentions and behaviour. The Theory of Reasoned Action asserts that attitudes (evaluation of anticipated behavioural beliefs) and subjective norm (the influence of important others with regards to a behaviour) concurrently affect behaviour (action inclination to carry out a behaviour). Intentions, in turn, are postulated to impinge directly on subsequent behaviour (Lac et al., 2013). The Theory of Planned Behaviour is essentially an extension of the Theory of Reasoned Action that includes measures of control belief and perceived behavioural control (see figure 1.). Perceived behavioural control (PBC) represents ones belief on how easy or how hard it is to perform the behaviour (Eagly and Chaiken, 1993, pp. 185). PBC is held to influence both intentions and behaviour. The addition of the PBC was added as there was a strong belief that it would help predict behaviour that was not under complete volitional control (Armitage and Corner, 2001). Thus, the inclusion of PBC gives information about the possible constraints on certain actions, as perceived by the subject, and it is held to explain why actions are not always a predictor of behaviour (Armitage and Corner, 2001).



Ajzen and Fishbein's 1989 Causal Diagram of the Theory of Planned Behaviour.

Figure 1.

2.1.2. PREDICTING BEHAVIOUR

There are several factors that can determine how likely it is that an attitude towards a behaviour will lead to the behaviour's occurrence. In simple terms, an attitude is more likely to affect behaviour when it is (1) strong, (2) relatively stable, (3) directly relevant to the behaviour, (4) important or (5) easily accessed from memory (Eagly and Chaiken, 1998). On the other hand, the above explained TBP would make similar assumptions based on the Figure x model. For example if someone who is constantly harming others online (let us call him/her a troll for the sake of the argument) reached the conclusion that their behaviour is really causing others harm (**attitude to the behaviour**) and believed that his/her peer group is not on board with this type of behaviour and would like it to stop (**subjective**

norm), and in addition, the troll itself believes that he can stop this type of behaviour due to their past behaviour and evaluation of internal and external control factors (**high behavioural control**), then this would predict high changes of resuming malicious online behaviour. In some cases, the model also predicts that perceived behavioural control can predict behaviour without the influence of intentions. For example if perceived behavioural control reflects actual control, a belief that the individual would not be able to exercise because they are physically incapable of doing so, would be a better predictor of their exercising behaviour than their high intentions to exercise (Ogden, 2004). Traditionally, TPB has been used in health psychology, for studies such as Schifter and Ajzen' s (1985) study on weight loss: results revealed that weight loss was predicted by the model; in particular goal attainment (weight loss) was linked to perceived behavioural control. One of the shortfalls of this particular model, which critics often debate, is the lack of a temporal element, the fact that there is no order in the different present beliefs nor is there a direction of causality (Schwarze, 1992). Online interactions are often affected by other circumstances. Normative beliefs in peer groups may be less inhibited in behaviour that is conducted via online mediums as some of the factor change, such as: lack of face-to face contact, time pressure for response, and so on – this is often referred to as online toxic disinhibition.

2.1.3. ONLINE TOXIC DISINHIBITION

Clinicians and researchers have observed how people appear to behave less inhibited when online as opposed to their usual offline behaviour (Suler, 2003). This phenomenon appears to be so pervasive that a term has emerged for it: "the online disinhibition effect" (Suler, 2005). When people show suppressed emotions, the go out of their way in order to help others, express fear and intimate wishes, we may call it 'benign disinhibition'. On the other hand, when individuals reveal

anger, become rude, critical, hateful and threatening or they simply visit places of perversion, crime and violence – something they would normally not explore in the real world, they display toxic disinhibition (Suler, 2005).

Whether online disinhibition is toxic, benign, or a combination of the two, when an individual loses its repressive barriers against underlying fantasies, needs and affect, one or two of the following factors account for this:

Dissociative Anonymity

This occurs whilst one's identity can be partially or completely hidden. Even though seldom information such as usernames and e-mail addresses may still be visible online (provided that they are not fabricated), they reveal little about the user. This anonymity is one of the principle factors creating the disinhibition effect. People feel less vulnerable about disclosing or acting out if they can detach their online actions form their in-person lifestyle and identity. Thus, the online self becomes a dissociated self (Suler, 2005).

Invisibility

This occurs as in most online environments as people cannot see each-other. Invisibility gives people the courage to say and do things that they would not say or do otherwise. They do not have to worry about the way they look or sound. Moreover, when 'invisible', people do not have to worry about the subtle, traditional signs of disapproval encountered in a face-to-face situation such as a frown, a sigh, a shaking head, a bored expression which usually inhibit what people are willing to express. In reverse, lack of eye-contact and face-to-face visibility disinhibits people (Suler, 2005).

Asynchronicity

One of the characteristics of the online environment is that communication is asynchronous. People can choose not to interact with each other at the same moment in time. Whether it takes hours to reply to a direct message on facebook, or days to reply to an e-mail, not having to cope with someone's immediate reaction disinhibits people. Some people might see asynchronous communication as 'running away' after posting a hostile message or making an important disclosure. Munro (as cited in Suler, 2005), an online psychotherapist, describes this as an "emotional hit and run".

Solipsistic Introjection

Online communication without face-to-face interaction can alter self-boundaries. It is not rare that people perceive their mind as having merged with the mind of their online companion. Reading someone else's message as a voice within one's head can feel as a voice within one's head, as if the other person's psychological presence has been internalized or introjected into one's psyche. Since one does not know what that person's voice actually sounds like or how the person looks, a voice and most often a visual image is assigned to that person, most of the times unconsciously (Suler, 2005). The online companion then becomes a reflection of one's needs and expectations. Once more, whilst in the safety of the intrapsychic world, people feel free to say and do things they would not normally say or do in the real world.

Dissociative Imagination

Some people, consciously or unconsciously, 'create' online characters for themselves and others which exist in cyberspace. Whilst this process gains magnitude in time, disinhibation magnifies it. People are still able to split online fiction from offline fact. Emily Finch (as cited in Suler, 2005), an author and criminal lawyer researching online identity theft, argues that some people may see their online life as a sort of game, where they have rules to follow and norms that do not apply to the real world. Once they left their desk and shut off their computer, they come back to their day-to-day routine, leaving their game behind and their persona within it. In this dissociative imagination, the express but split-off self, may evolve into a complex structure (Suler, 2005).

Attenuated Status and Authority

In offline, authority figures mostly express status in the way they dress and by their body language. The lack of that in cyberspace automatically reduces one's impact of their authority. In many online environments, everyone has an equal voice to express their ideas and desires, regardless of gender, race, wealth and generally their offline status. Since people are afraid to face disapproval or punishment, they become more reluctant to say what they really think when standing in front of an authority figure. Nevertheless, whilst online, in what feels more like a peer-to-peer relationship, where authority is minimized, individuals are more likely to speak out or act out (Suler,2005).

Individual differences

Individual differences play an important part in determining how and when people become disinhibited. Personality types have a great say in reality testing, defence mechanisms, and tendencies towards inhibition or disinhibition. For example, histrionic personalities tend to be very open and emotional, compulsive styles are more restrained whilst schizotypal characters are more prone to fantasy. Furthermore, the online disinhibition effect will interact with the before mentioned personality types, in some instances resulting in small deviations in the person's offline behaviour, whilst in other cases, leading to dramatic change (Suler, 1999). We, therefore, can say that any of the above factors leading to online disinhibition may also account or lead to forms of aggression.

2.1.4. DEFINITIONS OF AGGRESSION

Even though aggression is looked at as being a primitive instinct, modern society still experiences aggressions in its different shades and forms. Archaeological and historical evidence suggests aggression and violence was prevalent amongst the hunters and gatherers ancestor groups 25,000 years ago (DeWall et al., 2011). Aggression and violence was predominant in Greek, Egyptian and Roman societies up until as early as 2,000-3,000 years ago. Even though emancipation managed to reduce levels of aggression and violence in the modern society, this remains a ubiquitous part of human life. In order to understand why people react aggressively, violently or anti-socially, we must discuss the meaning of all of it (DeWall et al.., 2011)

Anti-social behaviour

Anti-social behaviour refers to any action that violates personal or cultural standards for appropriate behaviour (DeWall et al., 2011). Even though it often involves aggression and violence it is not always the case. For example if norms prohibiting intimate partners to punch bite or kick would be violated, this would be called anti-social behaviour. Even though behaviours such as littering, lying and stealing presumably do not involve aggression or violence they would still be considered anti-social behaviour. People suffering from antisocial personality disorder (Hare, 1996) frequently engage in aggressive and violent conduct, but they also violate standards for appropriate behaviour in non-aggressive ways, such as stealing, cheating and breaking other laws or moral norms. Therefore, anti-social behaviour can involve aggression and violence as well as any other type of behavioural response that defies societal standards for desirable behaviour.

Aggression and Violence

Aggression refers to behaviour carried out with the immediate (proximal) intention to inflict harm on another person who is motivated to avoid the harm (Anderson & Bushman, 2002) By exclusion, actions that are harmful by product of helpful, incidental or accidental , are not considered to be harmful (DeWall et al., 2011). In social psychology, the term 'violence' is used to describe severe types of physical aggression, typically the ones that are likely to cause bodily injuries. On some occasions, researchers will refer to non-physical aggression as emotional or psychological violence to underline the severe impact of actions. There are several factors that might lead to aggression - presuming that one individual is not suffering from any psychological disorder (that might lead to aggression) – ranging from mild triggers such as noise, heat, hunger, and ending with more serious

factors such as threat, fear or anger. Furthermore, research points out that males are more aggressive than females (Eagly and Steffen, 1986). More so, females tend to be less aggressive when they think their actions will physically harm someone, backfire onto themselves or cause them to feel guilt or shame (Eagly and Steffen, 1986). However, when discussing about aggression acts that do not cause physical harm, such as damaging people's relationships, males are not essentially more aggressive than females (Eagly and Steffen, 1986).

2.2. THE HIGHER EDUCATION ENVIRONMENT

The need for education has dramatically changed in the last decade as the demand for a highly educated workforce is increasing and young people are expected to undertake a continuous learning process (Aalavi and Leider, 2001). As a result, online learning is becoming an increasingly important part of higher education both on campus and in distance learning.

Information technology (ICT) facilitates economic, socio-cultural and educational transformation (Castells & Cardoso, 2000; Stehr, 2001; Robertson, 2005). It is looked at as being the pillar to supporting and converting the means of broadening access to education and transforming the knowledge access to the point where time and space no longer represent an impediment, thus the process can be undertaken whenever, wherever. This ICT phenomenon characterises learning and teaching as "the multitude of changes we face into comprehensible perspectives'' (Bell, 2001; Conole & Oliver, 2007). Especially in the Higher Education (HE) environment, it has brought major change in learning styles by use of digital devices in networked virtual learning environments (VLEs). Many studies have reached the conclusion that even though the internet has brought a revolution in

all the senses, it managed to change the way in which learners learn but not necessarily the way in which teachers teach in the HE environment. Nevertheless, more and more teachers are bringing new media into the classroom and studies of Facebook use in HE (Hewitt & Forte, 2006; Mazer et al., 2007; Tuncay & Uzunboylu, 2010, as cited in Wang et al. 2013) reveal a significant relationship between the Facebook use of college age respondents and higher motivation to learn, more effective learning and classroom climate, and improved faculty-student relationships. Perhaps that bringing new media into the classrooms is one of the reasons for its proliferation and the HE institutions have a direct contribution to the prevalence of cyberstalking on campus, thus both a moral and legal duty to adapt suitable regulations and police them too.

Half of this study revolves around a generation of students, born in or after 1980, a generation that grew up with access to computers and the internet and is therefore inherently technology-savvy. Today's student generation will be a lot different from student generations 10 or even just 5 years ago; more than a decade old data revels that students at the time spent less than 5,000 hours of their lives reading but more than 10,000 hours playing video games, 20,000 hours watching TV and an astonishing 200,000 emails and texts messages being sent and received, all of this before completing their studies (Prensky, 2001). The term "digital natives" was first proposed by Prensky (2001) to describe the above group. This group has also been termed as Millennials, or Net Generation. The core characteristic of this generation group is that they live their lives mostly immersed in digital technologies and they learn differently from previous generations of people. The new learning styles are said to include: "fluency in multiple media; valuing each for the types of communication, activities, experiences, and expressions it empowers; learning based in collectively seeking, sieving, and synthesising experiences rather than individually locating and absorbing

information from a single best source; active learning based on experience that includes frequent opportunities for reflection; expression though non-linear associational webs of representations rather than linear stories; and co-design of learning experiences personalised to individual needs and preferences" (Dede,2005, ap.10). Ardent debates are still being carried out as to if the brain structure of digital natives is different to that of other age groups and, and most research has failed to rule either for or against that theory. Nevertheless, Dr. Bruce D. Berry of Baylor College of Medicine states "*Different kinds of experiences lead to different brain structures. But whether or not this is literally true, we can say with certainty that their thinking patterns have changed*" (as cited in Prensky, 2001). We thus presume that digital natives will not only have different learning styles or thinking patterns but also they will look differently at any type of traditional authority when it comes to the World Wide Web. Another study of a student population on use of the internet, which fuels a desire of looking into the online norms of digital natives in higher education environments was conducted by Nagler and Ebner (2009) and concludes that rather than using the internet for photo sharing, bookmarking, blog reading/writing or YouTube, the so called net generation exists in terms of basic communication tools such as e-mail or instant messaging (online social networking platforms). Moreover, further similar studies have proven that even though raised in the digital age, most young adults are not highly knowledgeable about the Web (Bullen, Morgan, Belfer and Qayyum, 2008; Jones and Cross, 2009;Hargittai, 2010). Furthermore, data from The Higher Education Statistics Agency points out that the vast majority of students are either enrolled in distance learning or they are digital natives.

All of the people born before 1980, are referred to as "digital immigrants''. Pensky (2001) describes this group as adapting to the digital environment but they always retain characteristics, "accent" as Pensky describes it, of the pre-internet Era (i.e.

turning to the internet for information second rather than first, reading the instructions for a program rather than assuming that the program will teach them how to use it, asking for their secretaries to print e-mails instead of printing them themselves, and so on). There are three types of digital immigrants, the ones that do not believe that their students can learn in any other way than by traditional teaching methods thus they become frustrated when students lose focus; digital immigrants that do bring new media into the class but fail to use it, thus becoming vulnerable to student ridicule; and digital immigrants that have become technology-savvy and inspire their students to use new media in their learning (Prensky, 2001).

2.3. Defining the Problem – Prevalence of Stalking

Data from a CTIA's survey (CTIA, 2010) reveals that in 2005, there were 81 billion text messages sent across the network and 1 billion MMS. In 2010 the figures were; 2,052 billion for text messages and 51 billion for MMS. This represents an astonishing 2433% increase in text messages over a period of five years and 5600% growth in MMS messages. As technology advances, so do the means by which people cause harm and distress to each other but the awareness of harm does not necessarily change alongside, as a study by Short and McMurray (2009) points out strikingly, harassment was perceived as normality in their participants views: "*Stalking was not viewed as a serious offense in this form, despite the distress it caused to the victims, or expected from potential victims*." Within the United Kingdom, harassment accounted for 20% of police-recorded violent crimes in 2005/2006, although a breakdown of types of harassment was not noted (Walker, Kershaw, & Nicholas, 2006).

According to a study conducted by Finkelhor, Mitchell and Wolak (2000), 6% of their 1,501 sample of regular internet users aged 10-17 have experienced repeated online intrusions that had caused feelings of threat, worry or embarrassment. The reported incidents were akin for both genders and, moreover, 28% of the participants knew their harasser. In an attempt to develop a measure of cyberstalking victimisation, Spitzberg and Hoobler (2002) found out that a third of their study respondents (235 communication undergraduates) had reported some form of cyberharassment, which was judged to be benign. Nevertheless, 18% reported they had been "undesirably and obsessively" communicated with. Furthermore, a study conducted by Alexey et al. (2005) revealed that 37% of their student respondents have experienced a form of harassment and 3.7% of that group reported being cyberstalked. The group and sub-group were further analysed and data points out that there were a lot of similarities between the victims of off-line and online stalking. Most cyber-stalkers were former intimate partners or classmates of the victim. Also, cyberstalking victims were also likely to have been intruded upon off-line. Nevertheless, differences between the groups were also indentified: The authors learned that women were significantly more likely to report having been stalked (offline) whereas men were more likely to having reported being cyberstalked. When compared to proximal stalked victims, students were less likely to not respond to abusive communication and were less likely to call the police.

2.3.1. STALKING ON CAMPUS

Almost all HE institutions provide high-speed internet access in their residence halls. Some of these will also have Wi-Fi available. All universities with no exception (in the UK) provide computer labs and library computer access to all of their staff and students (Finn, 2004). Students stay in touch with tutors and family

via e-mail and most commonly nowadays, they communicate with friends via Instant Messaging (IM), which permits real time communication by sending short messages back and forth using the internet (Finn, 2004). On one hand internet use has many benefits that enrich students' scholarly and social life whilst at the university. On the other hand, there is evidence that internet use can result in negative experiences such as "cyberaddiction", identity theft, exposure to unwanted material, e-mail harassment, and cyberstalking (Finn and Bannach, 2000).

An earlier campus study conducted by Fremouw et al., in 1997 reveals that between 26.6% and 35.2% of female students and between 14.7% and 18.4% male students had been stalked (Fremouw et al., 1997). Furthermore, a National Institute of Justice (1998) study of 4,446 female students from over 200 universities in the United States found that 13% of women reported to have been stalked for a period of seven months in 1997 and 24% of all victims reported that the stalking included e-mail (Fisher et al., 2000). Finn (2004) reports in his study on a 339 student sample that 10%-15% of the participants reported online harassment either from a stranger, an acquaintance or a significant other. Furthermore, an impressive 58.7% of the studied population reported to have received unwanted pornography, which could be considered cyberharassment (Finn, 2004).

Many scholars argue that because of the developmental and mate seeking character of the student population and with the aid of the internet, Cyberbullying, cyberharassment and cyberstalking will remain a predominant problem to be understood, looked into and for which solutions should be developed (Ceyan, 2010; Finn, 2004). Although HE institutions are becoming more and more aware of these issues, there is still paucity in documentation regarding the extension of the problem in the UK, how students respond to issues when they occur and not to

mention the HE body's implication (Finn, 2004). Nevertheless, there is a continuous involvement form the HE sector to solve the online arising problems, which includes development of comprehensive Acceptable Internet Use Policies.

2.4. ACCEPTABLE INTERNET USE POLICY (AIUP)

It was over two decades ago now that figures such as Porter and Millar (1985) and Drucker(1988) first recognised that an '*information revolution*' was taking place (Neil et al., 2009). The aforementioned revolution not only had an immediate impact upon all aspects of organisational life but it still has significant effects on it today (Neil et al., 2009). This is an important concern for knowledge-intensive organisations such as universities, where computer-based information is becoming more and more predominantly needed in order to support teaching and admin activities, thus security breaches must be prevented and in order to do so, policies must be set in place (Neil et al., 2009).

There are numerous articles written about the need for policies in higher education institutions, in order to address issues and concerns surrounding the use of the internet by staff and students, but there is very little research based literature to cover the subject, most likely because of the innovative and recent characters of policies (Flowers and Rakes, 2000). These policies are now referred to as Acceptable Internet Use Policies (AIUPs) or Acceptable Usage Policies (AUP). One of the earlier quality documentations on AIUPs is authored by Day and Schrum (1995) who declare that sound AIUPs are needed to prepare educational institutions to adequately address rising problems of staff and students' internet use. Furthermore, to better illustrate the needs for policies, in 1998, Gaskin James writes a comprehensive document on the role of a policy, guidelines to writing an effective policy, and making use of such documentation. However, there are

earlier documented attempts of aiding policy making in educational institutions, such as policy templates and examples of policies (National association of Regional Media Centers, 1995; National School Boards Association, 1995; Perkins, 1993; Wentworth Worldwide Media; Wolf, 1994). If scholars identified the importance of a policy nearly two decades ago, underlining the legal liability on institutions, we can only presume that its importance has increased directly proportional with technological evolution. We live and work in a digital Era where devices connecting to the internet can be found in nearly every nook and cranny of an office or study environment. There is an increased awareness both in the public and private sector regarding issues surrounding internet abuse and its effects on institutional image, employee and students safety. In order to ensure that there is an acceptable conduct when using the internet within an institution, policies and procedures have been set in place. Policies are principles or rules that are intended to shape decisions and actions. Procedures are the ways that organisations implement policies (Consortium for School Networking, 2011). Whilst policies answer the "what" and "why" questions, procedures answer the "how", "who" and "when" questions. Usually policies are differentiated from procedures because of their need for a more flexible character.

The role of AIUP is not to control the user but to provide general usage guidelines (Kallman et al., 1996) Even though AIUP should be as comprehensive as possible, they should not be restrictive to the point of interfering with productive exploration or suffocating staff members (Siau et al., 2002). Usually most institutional policies follow the below guidelines:

- State the institution's values.

- The AIUP should complement the Code for Ethical Computer Use (might undertake different names in different institutions) and other codes and policies of the institution.
- Make it clear what purposes the Network can be used for.
- Emphasise that the institution reserves the right to monitor all forms of internet and e-mail use.
- Stress that transmission, display or storage of sexually explicit, defamatory or offensive materials is strictly prohibited at all times.
- Enforce policy in a consistent and uniform manner and assure disciplinary action will follow if there is a violation of policy.

(Siau et al., 2002)

A comprehensive study conducted by Siau et al. (2002) on three groups of organisations (Educational Institutions, ISPs and non-ISPs) reveals that most AIUPs are not formally worded nor legally sound. Moreover, none of the AIUPs reviewed in this study include a complete coverage of the internet abuse issues (see appendix 1) (Siau et at., 2002). We believe that it is of great importance that policies exist and they take the most comprehensive form they can, in order to eliminate any 'grey areas' and ensure that both staff and students are protected from any malicious online act and finally, ensuring that the university is covered in case of any lawsuit related to online misconduct.

2.5. SOPHISTICATION OF INTERNET USAGE (SIU)

Internet users become more and more reliant on technology, virtual communication became a common activity to them and an irrefutable fact is that individuals use the Internet differently (Hampton, 2007). That implies that each Individual using the internet will have a different set of skills and will employ it in

different ways. The lower end of the internet sophistication use scale will predominantly be held by digital immigrants who are still learning their way around the World Wide Web and at the higher end of the scale we will find the more technology aware, probably digital natives who use the internet in their day-to-day life. That is not to say that cultural, social and political circumstances will not contribute too. Furthermore, when we talk about sophistication of internet use this will refer to the time spent online, how much time is spent for each task, are tasks repetitive or not, and so on (Howard et al., 2001). In order to better understand human behaviour (online) – which has the same degree of complexity as the human mind - we must investigate the relationship between attitudes and behaviour. One of the lasting matters in Internet research is the 3W s issue: why individuals use the internet (i.e. attitudinal antecedents), how they use the internet (i.e. behavioural pattern) and what is achieved by using the internet (i.e. benefits/harm) (Peng and Zhu, 2011). It appears that since the operationalisation of internet usage is much more complex, the research process has undergone a change moving from uni-item measurement to multi-item measurement or more specifically from analysing how long individuals spend on the internet to how they spend their time online (Peng and Zhu, 2011). In communication research, internet use is operationalised as a time-based measure, which probably is inherited from the measurement of traditional media (Jung et al., 2001). In information system research, information system usage is mostly measured by a single item which examines the time an individual spends on a targeted technology (Sachez-Franco, 2006) or by multiple items which analyse the frequency and duration a person spends on a specific technology. Nevertheless, as pointed out before, an individual's cyber-life will not be monochromatic so the more time a social-demographic group will have to spend online, the more likely it is that they will use it in different ways. Therefore, before the time dimension, more valid measurements of the internet use will utilize multiple dimensions. On one hand

some studies took into consideration individual's skills of use (i.e. Thompson et al., 1994) or knowledge of the technology as a component of their usage (Rogers, 2003). On the other hand, some scholars divided online skills to four sub-dimensions: operational, formal, information and strategic skills (van Deursen and van Dijk, 2009). The current study uses the SIU scale developed by Peng and Zhu (2011), a uni-dimensional measurement model which was established based on confirmatory factor analysis. Furthermore, by confirmatory factor analysis, convergent and discriminant validity of the uni-dimension model is established within the multi-trait-multi-method (MTMM) paradigm. This particular scale was of interest as it shows that individuals' positive life outcome expectation, expected ease of use, and perceived popularity of the internet are significant antecedents of SIU with demographic characteristics controlled.

3. AIMS AND OBJECTIVES

1 Establish a relationship with the six selected universities, in order to create a favourable environment prior to conducting research.
2 Analyse the existing online acceptable behaviour policies, if there are any at all: How prominent are they? How much are they in accordance with the existing legislation?
3 Create a survey that will allow us to observe the incidents of cyberharassment and cyberbullying across the selected universities, both in student and staff members.
4 Conduct focus groups within the one institution to provide a more detailed understanding of the experience and attitudes towards online harassment and individual perceptions towards what is acceptable behaviour online.

5 Identify the level of awareness of any existing institutional policies amongst students and staff and analyse whether it acts as a deterrent.

6 Make initial explorations into the relationship between attitudes and online behaviour.

4. Research Questions

1. What is the prevalence of online harassment amongst people who populate the Higher Education environment?
2. Do Higher Education Institutions have distinct Acceptable Internet Use Policies in place?
3. Does policy awareness influence motivation to comply to acceptable online behaviour?
4. Identify the effectiveness of using an accepted model of social behaviour i.e. Theory of Planed B in online social behaviours.
5. Is there a normative explanation why individuals engage in online behaviour that distressed others?
6. Do young people follow any online norms? Which ones?

5. Method

5.1. Design of the Study

The present research uses a mixed method research design, more specifically, a triangulation design. The data will be collected both qualitatively (focus groups) and quantitatively (questionnaire), concomitantly, from different groups. Three groups have agreed to take part in the qualitative study. The focus groups will take part over two weeks, three focus groups per week, and again, the same participants for a second round of data gathering in the second week. The first

round of focus groups was designed to elicit online behaviour (appendix 2). Using this data, semi structured questions were designed for the second series of focus groups, in order to fill in the model of the theory of planned behaviour (appendix 3) . Semi-structured questions were used for the focus groups in order to get a better insight as it offers a more flexible way of gaining rich qualitative data.

Surveys have been categorised under four headings: factual, attitudinal, social psychological and explanatory (Ackroyd and Hughes 1983). Due to the specific aims and objectives of this study, a social psychological and explanatory approach was undertaken in designing the questionnaire (see appendix 4). Furthermore, the questionnaire was designed using the three different scales: the Classifications of Aggressive Online Behaviour Questionnaire (L. Sheridan, personal communication, 2009 as mentioned in Echo, 2011), the On Online Cognition (OCD) Scales (Davit, Flett and Besser, 2002), the Sophistication of Internet Usage (SIU) Scale (Peng and Zhu, 2011) as well as policy related questions designed by the researcher and supervisors. These will be used as tools to elicit internet behaviours and attitudes towards online norms and to get a better understanding of just how sophisticated the research sample is in terms of online usage. The current research addresses an interest in understanding both staff members of the HE environment as well as students' online behaviours but more so, their approach to institutional policy. All focus groups duration was between 45 minutes and one hour.

5.2. PARTICIPANT SAMPLE

5.2.1. STUDENT FOCUS GROUPS

The participants of the student focus groups were obtained convenience sampling. The sampling was mainly based on the convenience element, and could also be described as opportunistic sampling, i.e. not taken from the practitioners' population at large, but rather from a convenient subset of it (Dictionary of

Psychology, 2009). All of the participants are students of a digital media course, second level, at the University of Bedfordshire. Three different groups (of 5 to 10) students were agreed upon. Each group had attended two different focus groups, over two weeks. The aim of the first round of focus groups was to elude online behaviour whereas the aim of the second round was to go into details of personal experiences and attitudes towards the overall online environment so as to fill in the model of the theory of planned behaviour (see appendix 3)

5.2.2. STAFF FOCUS GROUPS

Data from a group of staff members at the University of Bedfordshire was also collected. Academic members of staff as well as administrative members of staff were invited by e-mail to partake in the study. The aim of the focus group was to discuss individual online experiences both work and non work related.

5.2.3. QUESTIONNAIRE

For the questionnaire, a convenience sampling was undertaken, making the study available both online and in hard copy. The questionnaire was filled in by both males and females of ages ranging from 18 to 65. The questionnaire has only interrogated students and staff members of higher education establishments so as the data is relevant to this study.

5.3. RESEARCH MATERIALS

5.3.1. FOCUS GROUPS

Materials used for the focus groups include a different questionnaire for each stage of the process. Separate questionnaires have been designed for week one and

week two (see appendix 5a and 5b). The questionnaires follow the structure of the session and are aimed at eliciting online behaviour and filling in the theory of planned behaviour model (Ajzen and Fishbein, 1980). Each focus group started with an icebreaker thus creating a more relaxed atmosphere and enabling the participants to share experiences. For the second week, the icebreaker was constituted of an online video (www.takethislollipop.com) which was then discussed with the participants.

5.3.2. QUESTIONNAIRE

For the survey, a questionnaire has been put together made up of 71 questions (see appendix 4). The survey has five main sections as follows: Section one aims at describing demographics, section two is a Classification of Aggressive Online Behaviour scale (L Sheridan, personal communication, 2009, as mentioned in Echo,2011) , the third section constitutes the OCS (Davis, Flett and Besser, 2002), section four represents another crucial scale in the process of determining online sophistication, namely the Sophistication of Internet Usage (SIU) Scale (Peng and Zhu, 2011) and lastly, the fourth section gathers data related to awareness of the AIUP within each individual's institution.

The Classification of Aggressive Online Behaviour Scale lists 11 examples of aggressive online behaviours (i.e. repeated unsolicited e-mail from one individual) and the participants were required to rate each statement on a six-point scale on how aggressive they viewed that behaviour to be (1= acceptable behaviour; 6=cyberstalking). The OCS is a 36 idem questionnaire that measures problematic internet use (i.e. I can't stop thinking about the internet). Participants rate their agreeableness on a seven point Likert scale of such statements. Furthermore, the OCS scores on four sub-scales (dimensions): Social Comfort, Lonely/Depressed,

Impulsive and Distraction. Therefore the scale will bring forward causes of looking at unaccepted online behaviour as acceptable Furthermore, the SIU scales is a 27 items questionnaire that measures online skill, online activity, diversity of online activities and time spent online.

5.4. PROCEDURE

5.4.1. FOCUS GROUPS

Participants will be invited to take part in a focus group, designed to understand their online behaviour. A semi-structured schedule will be adhered to, commencing with general questions relating to participants' use of social networking behaviours, such as: how the participants used social networking sites, who they generally communicated with and what is the style and frequency of posts they made. This will be followed by questions that address negative online behaviours. Examples, of questions asked include, "did someone ever post something (on your SNS) that made you feel uncomfortable?'' "Did you ever make any posts or comments online that you wish you had not?''. (See annex 3 and 6).
There are three distinct groups taking part in the study, and each group will attend two structured focus groups, each with a different purpose. To get a better representation of the structure of the focus group study, each of the groups was given a name (coordinate) W1A, W1B, W1C, W2A, W2B, W2C, where "W'' alongside the indicator stands for week one (W1) or week two (W2) of the study. The letters simply name each of the groups.

Within the first week a general approach is undertaken to elicit online behaviour. Even though not much discussion was encouraged on the acceptable use policy, it has been brought into conversation and participants were briefly questioned to test their awareness. Furthermore, all of the information gathered in week one

was used to create a viable and specific focus group design using behavioural examples, for the second week, which will help the researcher elicit specific information on behaviour that will ultimately fill in the TPB model. Whilst the second week's objective is to elicit behavioural intentions, it is also paramount that we do this in relation to the acceptable use policy of the University of Bedfordshire. Thus, some time was allocated to thoroughly discuss the acceptable use policy after it has been read to the group and all agreed to have understood it. Furthermore, risks/advantages of present legislation, perceived deterrents and perceived authority figures were discussed with the group, and notes of change in perception towards what is acceptable online behaviour and perceived barriers to behavioural intention as well as other variables have been taken.

5.4.2. QUESTIONNAIRE

Due to the specific aims and objectives of this study a social psychological and explanatory approach was undertaken in designing the questionnaire. The questionnaire was designed on a platform that allows users to create, run and analyse surveys, which is hosted by Bristol University and made available for students at the University of Bedfordshire (www.bos.beds.ac.uk). To facilitate access and ensure a high number of respondents, the survey was made available both in hard copies and online version (http://bos.beds.ac.uk/nccr). As mentioned previously, the survey comprises of 71 questions. Both students and academic/administrative staff of HE Institutions will be invited to answer the questions as accurately as they can, anonymously. The questionnaire will be available for the duration of a month. The survey has been shared online on social network platforms (facebook, twitter), by e-mail (sent from the Research Graduate School) and word of mouth.

5.5. ETHICAL CONSIDERATIONS

In order to carry out this qualitative research, an ethics form (see appendix 7) had to be submitted to the University of Bedfordshire IRAC* Ethics Committee, pending approval. This outlined the major aspects of the study and ensured that the participants were not placed within a research study that was going to cause them harm or distress. Moreover, mention whatever regulatory body IRAC/CST has.

Informed consent (appendix 4,5a, 5b.) - Consent has been given in a written format (both to focus group participants and questionnaire participants).

All participants have been given a consent form with a brief outline of the study. Signed consent will be required in order for the participant to be able to take part in the study. A separate sheet of paper that the participants can take away with them will enclose the researcher's contact details, contact details of the National Centre for Cyberstalking Research if they wish to assist in any further research project, as well as contact details for the National Stalking Helpline (http://www.stalkinghelpline.org) (appendix 4), should anyone need support. The participants are not from a vulnerable group and consent will be given from those participating and not a third party.

Confidentiality – Anonymity will be maintained throughout the study by not requiring any personal information such as name, address, phone number or e-mail address. Participants will be reassured that any information they give is confidential, cannot and will not be used to identify them and that they may withdraw from the study any time, should they wish to do so. The gathered data will remain confidential and stored within a locked cupboard on the university premises.

*IRAC – Institute for Research in Applicable Computing

Deception - Participants were informed that the study was in relation to their online behaviour and interactions, however further detail explaining that the fundamental assessment was on the relationship between known/unknown deterrents and their volitional behaviour, was not divulged.

Protections of participants – Since all of the participants were of age, there are no safeguarding issues involved. The levels of distress and discomfort were minimal as the topics of the study are not highly sensitive. Nonetheless, in the less probable case that someone did start disclosing, the person would have been informed that the researcher may not be able to keep the information to her/himself and will have to share it with the relevant authorities.

Following the completion of questionnaire, upon debrief or anytime following – should the participant require additional care, they will be referred to the university counselling services.

The right to withdraw - All participants will be advised prior to taking part in the focus group or completing the questionnaire, of their right to withdraw. Nonetheless, they can only do so up until the data is published. More so, the focus group participants may withdraw their testimony but any of the conversations that they might have enabled will still be used in the study. Each participant was asked to make a distinctive mark on their hard copies, in the eventuality that they wish to withdraw from the study and their data needs to be identified.

5.6. Data Analysis

5.6.1. Quantitative Data Analysis

The gathered questionnaire data was imported into SPSS to be analysed. For this set of data, the analysis was conducted in SPSS. Data from all of the four sections of the questionnaire was looked at separately, and then we linked scales to get an understanding of online behaviour and reasons behind unacceptable online beliefs. In terms of demographics, all of the participants were grouped into (1) members of staff and (2) students. In order to get a clearer overview of the data, for the first scale (Classifications of Aggressive Online Behaviour), all of the respondents were split into two groups; people who said that any of the listed behaviour was (1) Acceptable and (2) Sometimes Acceptable and a second group containing all of the people who said that the behaviour was (3) Mostly Unacceptable, (4) Cyberbullying, (5) Cyberharassment and (6) Cyberstalking. For the purpose of the research they were labelled as 'Group A' and 'Group U' respectively. Furthermore, for the last section of the questionnaire, related to policy, the respondents were again split into two groups; one group that knew about the policy (i.e. responded 'yes' to the question "Does your institution have a AIUP?") and a group that did not know about policy (i.e. responded 'no' and 'don't know' to the previously mentioned question). As the researcher has identified policies within the organisations of all the participants of the studies (see appendix 10), it is legitimate to claim that all of the respondents who said that their institution does not have a AIUP, were in fact wrong and lacked awareness of it.

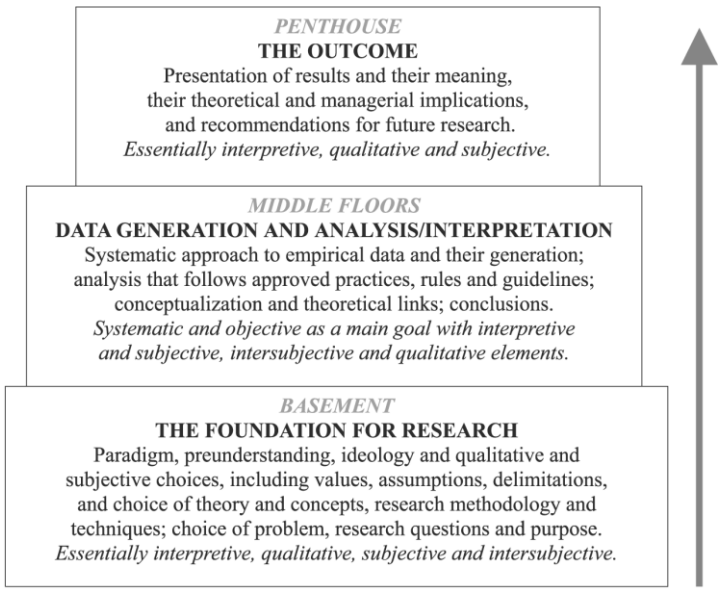
5.6.2. Qualitative Data Analysis

Thematic analysis was used for this particular data set. Full transcriptions of the focus groups recordings were completed (see appendix 8) when the questioning

process was over and data was analysed. To understand the analysis process better we must mention the word's origin, from the Greek language "analyein'', meaning 'to break up', or, according to Spiggle (1994, pp 492) to "divide some complex whole into its constituent parts". The analysis process as a whole represents dissecting a complex whole into minimal parts and reconstituting it to our own terms, more specifically, interpreting them. This was done by two researchers reading the transcripts together, by line basis and then identifying themes in the margin of the transcript. The researchers then agree the general themes and work together to establish the theme names. The researchers agreed on nine recurrent themes and worked together to establish the theme names. A benefit of this method is that it is not necessarily linked to a "pre-existing theoretical framework" (Braun & Clarke, 2006, p. 81), which differs from both grounded theory and interpretive phenomenological analysis but it can still be an inductive approach.

5.7. THE RESEARCH EDIFICE

With a background in both academia and private practice, and in an attempt to link the two sectors, Gummesson (2003) disputes that "all research is interpretative" (pp 482). He argues that regardless of types and context, whether academic or B2B, qualitative or quantitative, all research will follow the same paradigm, which he describes as a "research edifice" (see figure 2). Starting off from a perceived lack in research on the particularities of Higher Education Cyberharassment, the present paper undertakes the three stages of the research edifice model. Starting research with an understanding of the area, more specifically the cyberstalking problematic in nowadays' society, a concept for further in depth analysis of a specific sub set of the problem was created, namely cyberharassment and cyberbullying in HE environments. Furthermore, the data generation and interpretation stage was undertaken as described above. Presuming the data was analysed at its best and the most relevant information was extracted, the present work will draw from that, in an attempt to discuss implications and make recommendations for further research.



Source: Copyright: E. Gummesson (2003)

6. RESULTS

6.1. QUANTITATIVE RESULTS

Sample demographics

The Survey was filled in by 103 respondents which fit the survey criteria (all of them were affiliated to a HE institution, either as a student or a staff member). In terms of gender the sample was split evenly with 46.5% of the respondents being women and 53.5% men. Of the whole sample, 27.2% were members of staff, 28.2% undergraduate students, 31.1% postgraduate students and 13.6% being recent graduates. The respondents were between 19 and 58 years old, the whole sample having the average age of 28 years old. Furthermore, 70% of the sample was affiliated to the University of Bedfordshire (Luton). According to the Higher Education Statistics Agency (HESA), 56% of the total student numbers in the 2011/2012 academic year were women and 44% were men. Furthermore, 34% of the total student number for the same year was represented by postgraduate students and the remaining 66% being undergraduates. In terms of staff, there were 378,250 in the same academic year, which represents 9.5% of the total number of students that year. Thus, we can say that to a certain extent, our sample proportions of the demographic represents the HE.

Scale descriptive results

The Qualitative study made use of three scales. The first one, Classifications of Aggressive Online Behaviour Questionnaire (L. Sheridan, personal communication, 2009 as mentioned in Echo, 2011) was in fact an 11 idem questionnaire classifying attitudes to online aggressive behaviour, on a scale from 1 to 6 but based on perceived severity of the described act from Acceptable

behaviour (1) to Cyberstalking (6), therefore no reliability test was done for this section. The second scale used was the OCS (Davit, Flett and Besser, 2002). On this scale the authors reported Cronbach's alpha of 0.87 for Social Comfort, α = 0.77 for Loneliness/Depression, α = 0.84 for Diminished Impulse Control, and α= 0.81 for Distraction. Authors report a Cronbach's alpha of 0.94 for the overall reliability of their study. Following a series of reliability tests, for this scale, the current study scored a Cronbach's alpha of 0.90 for Social Comfort, α= 0.80 for Loneliness/Depression, α= 0.84 for Diminished Impulse Control and α= 0.84 for Distraction. The overall reliability scale for the current study was of α=0.94 (See appendix 12) . It can therefore be said that the results in this study are reliable. Furthermore, the third measurement scale used in the study was 27 items questionnaire measuring online skill, online activity, diversity of online activities and tine spent online. No reliability test was conducted for this measurement.

Policy and internet guidance

The questionnaire participants were asked the following Questions in relation to the policy:

(1)Does your institution have a policy on acceptable internet use?
(2) During your time at the institution did you have any guidance on how to use the internet?
(3)If not, would this be helpful?

Out of the 28 staff members sample, only 18 (64%) knew that their institution has an AIUP. Furthermore, from the 72 student sample, only 37 knew of the existence of an AIUP. Overall 55% of the respondents knew about the existence of a policy and the remaining 45% did not know. Out of the 67% (n=69) overall respondents

who did not have any guidance on how to use the internet, 61% (n=42) thought that any guidance on using the internet would not have been helpful.

General findings on acceptability of behaviours

First scale was used to measure how acceptable people find unacceptable online behaviour and test the reasons behind it. The respondents were split into two groups: 'Group A', the people who found the described behaviour either (1) Acceptable or (2) Sometimes acceptable and 'Group U' the people who found the behaviour (3) Mostly Unacceptable, (4) Cyberbullying, (5) Cyberharassment and (6) Cyberstalking. The results are as follow:

	Acceptable (A)	Unacceptable (U)
One individual seeking and compiling information about other individual and using it to harass, threaten and intimidate him/her on- or off-line.	**4.0%**	**96.0%**
Repeated unsolicited e-mailing from one individual.	**10.1%**	**89.9%**
Repeated unsolicited Instant Messaging from one individual.	**11.2%**	**88.8%**
Electronic sabotage such as spamming and sending of viruses by one individual.	**4.1%**	**95.9%**
Theft of the individual's identity by other individual.	**3.0%**	**97.0%**
One individual subscribing another individual to services without his/her knowledge or permission.	**3.1%**	**96.9%**
One individual purchasing goods and services in another individual's name without his/her knowledge or permission.	**5.0%**	**95.0%**
One individual using different identities in an attempt to contact another individual on-line.	**7.1%**	**92.9%**

One individual sending or posting hostile material, misinformation and false messages about other individual (e.g. to use net groups).	**3.0%**	**97.0%**
One individual tricking other internet users into harassing or threatening other individual (e.g. by posting my personal details on a bulletin board).	**3.1%**	**96.9%**
One individual making frequent (more than once a day) mobile phone calls or texts to other individual.	**16.2%**	**83.3%**

Figure 3. Quantitative results on perceived acceptable behaviour

The means of the two groups' scores were then compared with first and second scale, OCS and SIU respectively in order to get data on online behaviour.

Comparing Scales Scores

Firstly, we compared Group A and Group U's scores on the first scale with the OCS sub-scales using a T-test. Results showed that the scores for OCS total and Social Comfort were higher for Group A (respondents who marked unacceptable behaviour as acceptable). Thus people who scored high on OCS ($p= 0.012$) also have a high score for OCS Social Comfort ($p=0.002$). No significant results were found in the other sub-scales:

Independent Samples Test

		t-test for Equality of Means		
		t	df	Sig. (2-tailed)
OCSTotal	Equal variances not assumed	2.633	43.092	.012
Social_Comfort	Equal variances not assumed	3.289	44.373	.002
Lonely_Depressed	Equal variances not assumed	1.960	53.154	.055
Impulsive	Equal variances not assumed	1.978	42.091	.054
Distraction	Equal variances not assumed	1.940	51.046	.058

Figure 4. Quantitative Results on OCS Scale

Test results do not show a statistically significant difference in terms of online behaviour, between people that knew about the existence of the AIUP and the ones that did not know. Furthermore, no significant difference in terms of online behaviour was noted between people who had received guidance on using the internet and people who did not receive any guidance at all in that respect.

Furthermore, it was interesting to see how Group A would score on the SIU scale. We compared means by using a T-test. There was no significant difference between Group A and Group U in terms of online sophistication and time spent online, although, Group A have a statistically significantly higher score (p=0.042) for the online activities aspect:

Independent Samples Test

		t-test for Equality of Means		
		t	df	Sig. (2-tailed)
Online_Skill	Equal variances not assumed	1.293	72.771	.200
Online_Activities	Equal variances not assumed	2.096	44.241	.042
Diversity_of_online	Equal variances not assumed	.251	86.120	.802
Time spent Online	Equal variances not assumed	.277	46.659	.783

Figure 5. Quantitative results on SIU Scale

No significant results were found when the group that scored higher on Social Comfort was lined to the SIU scale. Moreover, there were no statistically significant differences between staff and students in terms of behaviour of use of the internet.

6.2. QUALITATIVE RESULTS

Below are presented the results for the first round of focus groups (three different groups adding up to a total number of 25 participants). It should be noticed that all of the participants confirmed to have access to a computer/desktop/mobile device; they all use the internet both at home and at university (University's Wi-Fi). Furthermore, all of the present ones have an account on a social media platform (i.e. facebook, twitter, beebo, instagram, etc.), which they use for diverse purposes. A further analysis of the first set of data which was meant to elicit online behaviour was conducted and the following themes have been identified:

6.2.1. QUALITATIVE DATA WEEK ONE FOCUS GROUPS

A. CONCERN ABOUT WHO THEY APPEAR TO BE ONLINE

Data indicates towards the fact that there is a string perception of online characters amongst the interviewed population. All of the respondents have agreed that it is important how people perceive them online and they have to be careful about what they select to represent them on their various social networking profiles:

> " *…you have to carefully select it because it is there for everyone to see. So you want to make a good impression, something like that. I think it happens subconsciously".*

When asked if they create an online persona, some of the participants responded yes whilst some declared:

> "*…you just select some parts of your personality and expose that".*

This is a recurrent theme across the transcripts, participants who have an understanding of the online environment and express the belief that *"facebook (online environment) has evolved…you have to think about your business and be careful about what you post online".*

"in terms of posts, I think it is very important not to post every bit of thought".

Furthermore, one participant agreed that his online appearance is mostly dictated by other people as he is being tagged in pictures which he would not say is how he likes to be perceived but at the same time he likes them so does not want them to be removed "I think I would probably notice that 95% of my pictures on my

facebook are of me being drunk or are related to alcohol consumption''. Another participant confessed that he felt embarrassed by past online presence as this does not represent him anymore "It is embarrassing. And then I delete everything''. All of the above only further prove that young people are indeed concerned with the who they appear to be online, in most cases they are aware that their self image is temporary and will most likely change in time but nevertheless, as further analysis will point out, they still believe that the online environment is not "such a serious matter'' which may point out that they are not fully aware of any long term repercussions related to the way they speak and appear online.

B. ALMOST ALL UNPLEASANT EXPERIENCES HAPPENED IN ADOLESCENCE

It is worth mentioning that the age group of these focus group participants is between 18 and 22, thus their recollection of adolescent experiences is fresh in their memories. All of the participants talking about different negative online experiences confess that they only happened when they were in school/college and not the present time, they believe they are more mature and do not experience cyberbullying anymore:

'It is definitely a more mature environment, as we do not bully each other as we used to do in high school'' .

More so, even if now they experience mildly negative online experiences they treat them differently as they confess to have more knowledge about the internet and know that people only say "mean stuff'' online because they experience a perceived power given by the fact they are behind a desktop rather than face-to-face.

"When I was in high school, you would find out what people say on facebook from other people. It is not necessarily bad stuff, it can be funny stuff or… but people talk".

"Yes, you would hear about people's identity. You can't be in high school and never hear a rumour about someone to be honest, cause you are surrounded by rumours all the time".

Another finding on this particular theme was that female participants reported more frequent malicious communication in the online environment (mostly bullying) than male participants did.

C. NOT TAKING THE ONLINE ENVIRONMENT TOO SERIOUSLY / POSTING SOMETHING YOU THEN REGRET

Another interesting fact that the data reveals is that young people do not take the online environment too seriously, which may or may not be the reason why they sometimes post things that they regret.

"Have we not all posted something we now regret? I have".

"It was meant to be a joke, but looking back now, I regret having done it".

"It is stuff you regret but it's not awful. You put something on and then you look back the morning after and you ask yourself why you put that on. But it's not mean, it's just embarrassing yourself".

When asked how they felt about someone else posting on their behalf on a social networking site and if they thought it was a bad thing, they did not believe it was that serious if a close friend had done so.

"If it's a close friend I would not mind that, but obviously if they are strangers…''

Furthermore, they would find it unfit for a stranger to engage in such behaviour but not too serious:

"It is not really something serious so it's not something you should be sympathetic about''.

"You just do it and then you think why did I do that? You do it to someone you know and you mock them for not being careful with their phone. Lack of common sense''.

Moreover, aside the mild cases of online bullying, three participants have disclosed their online experiences (from high school) which did seem more serious and other parties were involved such as police, school management and/or parents. One of them was aware of the reason behind that type of behaviour and had consciously started it up whilst in the other two cases the reason was not known. One of the three cases in particular proves to be more serious. The male participant describes being threatened online by another group of male students, with no apparent reason. He said he did not think that there was anything else he can do about it except not to engage. The participant states that the threats stopped after a few weeks as he was not responding to either of their messages (sent on beebo). Around the same time, our participant found out from school management that the same people that were causing him distress were now arrested for murder. From what he knows, they choose to pick up on another student from a different educational institution and threatened him in the same fashion only that this time their threats materialised.

"I only then realised how serious the situation was and that I should have let someone know about what was going on but, I was young…what did I know?"

D. REACTIONS TO NEGATIVE ONLINE COMMUNICATION

When discussing how participants would react if they saw an offensive post on their news feed, or whether they engaged in such posts or posted them themselves, the opinions and experiences were diverse, ranging from people saying they would never interfere in a public conversation that had an offensive character or might go that way, to people saying they would and have intervened in the past, trying to ameliorate a situation which had gotten out of control:

"There was this girl in my high school and we started making fun of her on facebook… there was someone that actually said guys, you are crossing a line and then everyone stopped with the nasty comments. We realised we had gone too far".

"Sometimes I hold back or sometimes I would say 'you should not say that, this is stupid'. People always find out these kind of things, cause people talk to each other".

"The only case I would say something is if they say something stupid or insolent, I would say something. This is really the only case you can say something".

When asked if they would tell a friend that his/her online presence is sending out a wrong message, everyone agreed that they would do it but privately, in order to protect their reputation. When asked if they would intervene in a conversation where one of their close friends was bullied by another close friend, they said:

"I would probably just talk privately with them. If it is something that would make one of your friends look back, you would not add fuel to the fire. So you take it somewhere else. Privately".

"If it is someone that I do not particularly like, I would not go out of my way to save them".

E. PEOPLE SEEK ATTENTION, THEY INVITE NEGATIVE ATTITUDES

Interestingly enough, the above discussions on intervening to stop malicious online behaviour lead to discovering that most participants and all female participants of all of the focus groups, believed that some people deserve to be bullied because they themselves seek attention.

"Yes, people might deserve what they are getting. Some people post stuff to seek for attention. They intentionally invite people to have an argument. Like some people would post something good heartedly and others would be bastards".

"If there is someone that is constantly posting crap then I would probably like to see it blow up in their face. Cause people that just post rubbish are quite annoying. But then good heartedly people that just post an opinion and it blows in their face, I think that is quite different. I think it depends on who is being bullied".

"Yes, it looks like you are destroying your privacy. Because you reveal everything about you".

"In some cases it is almost like girls invite for rape".

Another interesting belief that came about in one of the larger groups, where the mix was more homogenous (approximately equal numbers of males as females) was related to gender. All of the participants, women especially felt like they (women) are in a more delicate situation than men are, when online. They think to be perceived as being weaker thus easier to approach with dubious intentions. Moreover, there was a general consensus on the fact that males should deal with whatever issue they are facing on their own, that because they are men they should have the coping mechanisms and be able to resolve any online refute that might lead to cyberbullying or cyberstalking. Not all that surprising, men agreed to the previous statement.

F. ONLINE NORMS ARE COMMON SENSE

Another strong theme that came up during discussions was that online norms, at least for this age group (digital natives) are common sense and everyone should know and feel what is right and what is wrong, just like they do in their day to day lives.

"A few years ago, there was this guy that said something like 'I hate Islam'. Now, you just cannot say that sort of thing on facebook. I don't think people think as they should do, when they post this kind of thing".

All participants were asked if they had ever had any workshops, training or any other sort of guidance on the use of the internet and social media platforms during their years as pupils/students. In two out of the three groups there was one person claiming to have had guidance from parents and two claiming to have had guidance from their teachers in high school, the rest, approximately 19 participants have never had anyone telling them how to behave online or what to be careful about when interacting with strangers online.

"No, there was no-one telling me how to use the internet. But I think it's common sense. You know all those things you were told as a child, I think you can apply all of those to online social networking''.

"My beliefs are similar except that we have been told in school about the dangers of social networks. General stuff like don't accept people you don't know''.

"My parents told me to be careful with what I post on my page and do not accept people I don't know''.

"I don't think I would reveal my personal information online. I think that comes to common sense again''.

Most of the participants had their beliefs enrooted in their previous experiences thus saying that as you grow older you learn how to behave in an online environment without having anyone telling you how to do it:

"I think as you get older you realise the things you should and should not do online, but I think that when we are younger we should be told about the dangers of the online environment''.

Participants felt that when young and less knowledgeable they were more vulnerable to cyberbullying.

G. EASILY ADAPTING TO ONLINE PLATFORMS / USING SOCIAL MEDIA AS A LEARNING TOOL

When asked about privacy settings on their accounts, all of the participants confirmed they did customise their privacy settings on all of their social media

accounts. When asked if they have done so because of something they might have seen in the media or if it was an instinct, most of the respondents, with a couple of exceptions, said it was instinctively *"I would have done it anyway"*. Two students said they have done so because of their parents' *"nagging"*. They all expressed being knowledgeable in terms of operating on all of the social media accounts they have and said to have learned this fast as they were interested in *"knowing how to do stuff"*. When asked what type of communication they use for university related work, the answers were: facebook groups and mobile messaging:

"Everyone uses facebook, it's easy", *"Everyone checks their facebook at least once a day"*.

"I actually have a facebook group for one of my projects. We use it to get in touch with each other and arrange meetings. I think it is useful".

"It is helpful at times (facebook) if people actually bother to respond".

H. LACK OF AWARENESS ON POLICY AND TERMS AND CONDITIONS AND EXPECTATIONS

Participants were first asked if they knew of any documents that regulate online usage to which they all replied no. Then they were asked if they think there should be something to regulate the use of the internet, for example, here at the University of Bedfordshire, if that would make them feel safer online. More than half of the participants said no, and cared to argue their answers:

"I don't think such a policy would prevent anyone from doing anything. I think no one would listen if university would say you can't do this and can't do that".

"I think it would have the reverse effect. If university tells you not to do something, then you want to do it''.

When asked if they know university has an acceptable use policy, for their Wi-Fi and internet, most of the participants said no. The ones that said yes, they knew there was *"something you have to agree to when you log onto the Wi-Fi''* network but they did not ever read it:

"No, I didn't read it but it's common sense. You cannot go online and do all sorts of stuff in public!''

"To be honest, these days, who reads terms and conditions?''

"We don't do it just because generally people can't be bothered''.

"Even when I signed for facebook I didn't read the terms and conditions cause I didn't care''.

Furthermore, a hypothetical discussion started based on what participants thought the policy should contain (since none of them has read it, they could only guess what it says).

"I think it says it is your responsibility what you do online and that they can track you down if you misbehave''.

"I think this may also be related to sites that use your personal information such as your bank card details and other related''.

"I think we would all expect to find some advice on how to use the internet adequately".

"I don't know, I would expect to find a lot on how to conduct yourself on social networking sites to be honest".

"I am pretty sure you cannot add any of your teachers on facebook until you are out of university. As in graduated".

The students have had a class where they read though the facebook terms and conditions, as part of their curricula. It was interesting to find out how their behaviour changed once they became aware of the terms and conditions of using that particular platform, information they did not have prior to that class. The groups were asked if they changed their behaviour after they read thought the terms and conditions. Most of them said yes:

"Yes, I often tell people that actually their pictures are not theirs anymore. I told my parents that and they were really shocked."

"It shocked me too! Well, I knew that they are withholding your information but…"

"Facebook knows that not a lot of people are going to read the terms and conditions so they could be putting anything there."

Week two focus groups were slightly different in approach, as the purpose of the sessions was to elicit specific information to fill in the model of theory of planned behaviour (see appendix 5b). Furthermore, the second part of the focus groups focused on policy related.

I. DISCUSSIONS ON POLICY

As part of this research exercise, the acceptable use policy of University of Bedfordshire (see appendix 9) was read to each of the groups so as a more comprehensible conversation could be carried forward. As mentioned in the previous data set, when the policy issue was briefly brought into the matter, the majority of the participants were not aware of its existence nor knew where to look for such a document and furthermore, even the ones that did know that regulations might be in place, have never read it. The question was asked again and the answers were the same.

Q: So what do you think about the text that I just read?

R: *"I don't agree with it. Having policies. Especially when going to uni. If you are an adult why would they put all of these regulations in place? If that is how you want to spend your 9 grand….Obviously you come here to get a degree and move your way up into the world so if you wanna come here and spam people for 9 grand and then get kicked out of uni…is that person's issue."*

R2: *"To an extent, you can do whatever you want. But there are so many ways you can dodge the rules and laws and whatever. I think it's just up to the person."*

R3: *"I think people pretty much ignore it. Young people post anything without thinking or caring."*

When the first focus group participants were asked whether they felt bound by the policy in any way, or thought it acted as a deterrent, they all shook their heads.

"Before today I did not even know there was one so…"

"I think it has no power whatsoever.''

"*I don't see uni as too much of an authority figure. Cause it's optional, cause I came to them…''*

The second and third focus group participants were able to see how this policy might play an important role in policing online behaviour within the university but they were not entirely convinced that this would act as a deterrent, mostly because of lack of awareness and the fact that there are no sanctions mentioned.

"I don't think this would stop people. Everyone would still find a way to do whatever they were doing.''

"Then again there is nothing to say 'failing to comply with this will bring sanctions…'.''

"*Yes, by not having any sanctions on it, it makes it less credible, to me it just proves that they made it to scare people.''*

"I think it's there just to inform people.''

All participants felt that the policy was a rather relaxed and to them it constituted no deterrent to their online behaviour on the universities premises, whilst using its network. Nevertheless, they all came back to the issue of morality and common sense "you would not do this, you don't need a document to tell you that is bad'', believing that they are fully capable of controlling their behaviour and act in such a way not to cause anxiety to anyone around them.

6.2.2. QUALITATIVE DATA WEEK TWO FOCUS GROUPS

In week two, a process of determining specific behaviour to fill in the theory of planned behaviour model (figure 6) has been undertaken, by asking specific questions.

POST 1. MATT

POST 2. SKYLAR

Figure 6. Facebook posts, 2013

Belief Strength

In order to elicit how strong participants beliefs are, questions starting 'How strong do you believe that…?' On a scale from one to five where one is not confident at all and five is really confident, all participants rated their confidence towards retaining

from engaging in unacceptable online behaviour on 4. The same belief came out of the further discussions in the focus groups.

Belief evaluation

In order to measure the participants' beliefs, questions such as "Do you believe this behaviour is acceptable? Why?'' have been asked.

All participants found the first post acceptable whilst they thought the second one brings serious offence and should not have been expressed in a 'public' place:

"I think it is ok for the first one to be online cause it is more like a joke. If I would see that online I would laugh, they need to grow up.''

"The second one, no, I don't think it's acceptable at all, especially since there are a lot of young people killing themselves.''

"The first one I think it's quite acceptable, it's funny, it's just a petty argument.''

"In the first post they have a lover's quarrel, whilst in the second one they refer to somebody else, and that is not right because they cannot judge people like that.''

There was a general perception that when an online post refers to you and your circle of friends it is ok to be direct whereas if you are expressing strong opinions on gender issues, religion, politics or any other matters that concern a larger population sample then it becomes unacceptable online behaviour:

"I think the second one is crueller as it affects a wider range of people whilst the first one…''

A couple of participants bought the freedom of speech issue into the matter arguing that if you would shout something in a square, and it was mean to others, why would you not say it online?:

"As stupid as the post is, they would say 'freedom of speech'".

"I still think that everyone is entitled to an opinion but you cannot express it like that.''

Attitude

Participants were asked what their attitude is towards this type of behaviour. Whilst all of them thought the second one was of a higher gravity than the first one, a third of the participants thought the second one was funny and they could see themselves engaging in similar behaviour. Nonetheless, they all said they would ignore the first post completely. Furthermore, the opinions were not much different regarding the second post meaning that most participants would not engage in that type of discussions in any way nor would they post such a comment.

Normative Belief

In order to reveal participant's normative belief, questions such as "What do your peers think about this type of behaviour?'' and "What do you think authority figures in your life think about this type of behaviour?'' were asked.

Most people said that their friends would believe the same as them with regards to the first post:

"The first one I think it would be more acceptable to my peers than the second one".

When asked who represents an authority figure in their life, participants said: parents, friends, sister, brother, police, university. Whilst only a limited number of participants saw university as an authority figure, all participants see friends as an authority.

Motivation to Comply

Participants were asked what would be the risk of this type of behaviour in their peer group (second post type of online behaviour), if there would be any benefits of such conduct and if they perceived any type of deterrent to this type of actions.

Most participants said their friends would not be happy if they would show signs of aggressive online behaviour:

"My friends would not be happy. They would contact me, ask me why I did do it and ask me to take it down".

Nevertheless, there were also people saying that:

"My friends would not say anything. I don't think my friends would ask me to take it down. Maybe someone acquainted might say to take it down..."

Almost all people said there would be no major consequences for not following their friends '*advice*':

"They would not ignore me if I refused their advice, they would carry on stressing their point until either I listened or I distanced myself from them."

And once more, when asked about any impediments in posting any such a comment, they all saw none. Moreover, they invoked the *'freedom of speech'* argument as well as the fact that facebook is not being policed by anyone and much worse posts/videos/pictures get uploaded everyday without being anyone to take them down.

Subjective Norm

In order to elude subjective norms, participants were asked, within their peer group, what would most people do? Would anyone engage in this type of behaviour? (the second post). Whilst almost everyone said their friends would not post anything like that, there were a couple of participants saying their friends would:

"Yes, I do have friends that would post that without thinking. They are a bit stupid."

Furthermore, another case was made in one of the focus group, that not all of the people they have as friends on facebook are really their friends, but mostly acquaintances. Whilst they affirmed that their friends would not engage in similar behaviour, they said that some of their acquaintances might do, but that does not represent their beliefs.

Control Belief

In order to see how participants perceive their control, they were asked how easy it was for them to know if they are causing revulsion, anxiety or annoyance to anyone else?

When discussing this particular aspect, the opinions were widespread. Some of the participants thought it was a matter of common sense, whilst other believed that it has a lot to do with personal beliefs and personality "so it is difficult to say when you are annoying someone". While the general belief was that *"it depends on each individual's tolerance and personality''*, there were couple of participant that had identified the hollowness of the written messages in terms of emotions:

"Sometimes it is difficult to interpret things in writing. Because someone could be meaning something and then someone else could take it as something different.''

Perceived Power

This part of the questioning was design to analyse if participants could anticipate their behaviour (i.e. How confident are you that you could anticipate how your behaviour will be experienced).

Whilst most participants said they could anticipate how one of their posts would make people feel (partly because all of their posts are very neutral, i.e. sharing music), there were participants that said they could not anticipate how their online behaviour would make someone feel.

"People have different opinions so there could be someone to disagree no matter what you say, in every post you put so…''

"*Some people might think about that type of things but some will not. Considering others.''*

"Personally, I don't think my posts over but at the same time, I don't want to offend anyone. Like send subliminal messages or anything.''

Perceived Behavioural Control

Keeping in mind the second facebook post, the participants were asked how confident they were that they could control their online behaviour and reactions in a similar situation. Most participants said that if they would ever get caught up in similar arguments they would rather leave the conversation altogether than start an argument. Again, participants believe it has everything to do with personal views and personality type, that if some people like to stir things up they will find a reason to engage in aggressive online behaviour but "*if your views do not match my views, I would just leave it at that''*. Participants admitted to holding back from interfering in such posts as they fear that they might get bullied if they were to say something, good or bad "*usually that is what happens''.*

"Some people are very defensive of their opinions, and it's easier to be nasty about it on facebook because you are not doing it face to face but online''.

"*Yes, because they are online they can be nasty''*.

Some participants said that if anyone would take one of their posts astray and cause distress, they would block them. None of the participants considered reporting such behaviour would do any good as facebook was not strict enough and not policing their platform enough.

Behavioural Intention

At this stage there was an interest in finding out if in similar circumstances (if or when they have strong views), any of our participants would engage in any of the behaviours illustrated in the post, including comments. If they said no, they were asked what they would do instead.

All participants stood by the fact that they do not have any strong views and do not feel a need to express any even if they did have them, as they believe online is not the right place to do that:

"with certain things you have to tip toe, you can't be that direct especially in today's world".

More so, participants added that they might post something harmless which could then escalate, which some thought was the case of the second post. Meaning that in their view the post was not all in all so awful but as more people engaged and supported the attitude, the post got nastier:

"I think your post can be driven in any direction by your facebook friends. No matter how positive or negative it seems, it has the potential of growing into something much more and it could lead to hostile behaviour.''

Volitional Behaviour

Participants were asked if they ever engaged into this type of behaviour, if they ever cyberbullied someone or posted hostile material. All of the respondents said no.

6.2.3. QUALITATIVE DATA FROM STAFF FOCUS GROUP

In order to get a 360 degrees feel of the online experiences on campus, data from a group of members of staff was gathered. Half of the participants are academic members of staff and half of them are administrative members of staff from different departments across the university.

As you will be able to see in appendix 8, all of those present in the room, have had negative online experiences. Whilst all their experiences varied in intensity, they all had the potential of harming a group or the institution as a whole, rather than a single person. Furthermore, it appears that the most often online negative experiences were related to the use of internet; most situations revolved around breaking into e-mail addressed and distributing classified material to an entire address book, or simply spamming. Even though these experiences were not seldom nor were they mild in character, the participants reported there is no protocol in place, for dealing with such events and usually when something like this does happen they just '*play it by ear'*. Furthermore, members of staff reported that at times there can be tense communication amongst themselves and this is mostly due to the fact that written communication is very different than face-to-face communication:

"…this member of staff constantly bullies me though e-mail but when he comes to my office he's like a puppy. Of course, when he talks to the screen he can be more… but when face-to-face, he would not dare to say those things."

"I think the internet gives you the false perception that you can hide your identity."

"I think with e-mails and all that is written basically, you can say so many things in so many ways and when reading it, you might misinterpret what the person wants to say."

All participants reported having accounts on social media platforms but because of the rather limited interactions, they did not experience as many unpleasant events as the students might have. When asked if they would know what to do and who to go to in the eventuality that they were cyberharassed, the women almost instinctively said no, whilst all of the male participants had an answer of their own as they were not sure if there is a protocol to be followed in such situations. More so, when they were asked about the acceptable use policy, only a third of them were aware of its existence, knew where to find it and what it means (this might have been due to the fact that they are academics in the Computer Science and Technology department).

7. DISCUSSIONS

The primary aim of this study was to find a connection between online behaviour of the HE population and awareness on the existence of AIUPs. Furthermore, the study also set to discover whether there are any norms HE population follows and elucidate them. But mostly, this study seeks to understand why students engage in unacceptable online behaviour and what influences this type of behaviour.

Qualitative data gathered in this study shows that online harassment is more acute in adolescent years rather than at university. Virtually all focus group participants reported negative online experiences during their time at high school. Furthermore, female participants reported more negative experiences than the male participants, which was mostly cyberbullying. This finding is consistent with a study conducted by Rivers and Noret (2010) on a young population (11-13 years) of nasty/threatening emails and text messages. Their study reveals that over a five year period, the number of students experiencing nasty communication increased significantly, especially among girls. Furthermore, most participants knew their harasser/ bully - this finding is also consistent with a study conducted by Prenski (2001) on a 1,501 sample of regular internet users aged 10-17. Their data shows that all 6% of the participants who reported having gone through negative online experiences knew their harasser. Nonetheless, all focus group respondents believed that now that they are at university (and being of age), they think and act more maturely and also, they have not experienced any unpleasant experiences during their time at the university so far. It should be mentioned that the sample was a second year group; with ages ranging from 18 to 22, therefore, their recollection of high school events is still fresh. On the other hand, being only half way thought their university years, they have not yet experienced all that there is to experience, including possible arising negative online experiences. Furthermore, members of staff reported mild online aggressive behaviour which they considered to be due to the fact that face-to-face interaction was lacking and it was easier to say mean things "when behind a screen" – this aligns with Suler's (2005) reasoning on online toxic disinhibition and similar findings of a Lapidot-Lefter and Barak (2012) study on anonymity which concludes that lack of eye-contact was the chief contributor to negative effects of online disinhibition. This particular motif was recurrent throughout the student focus groups too. Furthermore, another motif of

both staff and focus groups was the fact that written language can be easily interpretable – this is tangential with some of the findings Douglas and Sutton (2010) reveal in a study on power of language. They argue that people may not always be aware of their linguistic choices.

In order to offer protection to the HE population from online malicious communication and prevent negative experiences, universities develop AIUPs. Some are more comprehensive than others or they might come under different names (Acceptable Network Usage, Acceptable Usage Policy etc) and some may not be distinct but as far as the sample of this study goes, AIUPs exist. In spite of the prevalence, the researcher has identified policies within the organisations of all the participants of the studies (see appendix 10). It seems that raising awareness about AIUPs is not a high priority in most universities as qualitative data reveals that almost none of the students at the University of Bedfordshire were aware of its existence. More so, none of the participants have ever read it. Even though there are quite a few studies discussing policy making and analyzing different types of institutional policies (National association of Regional Media Centers, 1995; National School Boards Association, 1995; Perkins, 1993; Wentworth Worldwide Media; Wolf, 1994, Bradbard et al., 2010) no study on policy awareness was found by the researcher. However, quantitative data reveals that 55% of the respondents knew about the existence of AIUPs at their institution. Out of those, 17.5% were members of staff.

Once all of the focus group participants were informed about the AIUP (this was read to them) they were questioned to see how the awareness would influence their behaviour. Most participants said that their behaviour will not change in light of the newly acquired awareness on the AIUP. The fact that they now knew about existing regulations does not appear to have changed their motivation to comply

to acceptable online behaviour. Participants declared that they do not feel bound by the AIUP nor perceive it to have any power at all. There was a perception that because university "is optional" and they chose to be at the institution, no such rules should be enforced, not to mention punished. Furthermore, only a third of the staff members that took part in the focus group knew about the existence of an AIUP. The high number of members of staff knowing about the policy might be explained by the fact that more than a third of them were part of the Computer Science and Technology Department thus they have more involvement in the technical aspects of internet use than most academics or non-academic members of staff. Quantitative data did not reveal any statistically significant relationship between the people that knew about the policy and aggressive online behaviour.

This study preponderantly seeks to find out the reasons for which students engage in unacceptable online behaviour and what influences this type of behaviour. The best method for answering this question was to gather data and apply it on a consecrated behavioural model and asses its effectiveness. TBP was one of the most suited theories to aid the current research. The TPB has received considerable credit in (social) psychology literature as it brings forward an integrated model of behaviour and it is one of the most widely researched models. It was developed to explain how persuasive forces and motivational beliefs drive intentions and behaviour. TPB asserts that attitudes (evaluation of anticipated behavioural beliefs), subjective norm (the influence of important others with regards to a behaviour) and perceived behavioural control concurrently affect behaviour (action inclination to carry out a behaviour). Intentions, in turn, are postulated to impinge directly on subsequent behaviour (Lac et al., 2013). Perceived behavioural control (PBC) represents ones belief on how easy or how hard it is to perform the behaviour (Eagly and Chaiken, 1993, p. 185). PBC is held to influence both intentions and behaviour. Thus, the inclusion of PBC gives

information about the possible constraints on certain actions, as perceived by the subject, and it is held to explain why actions are not always a predictor of behaviour (Armitage and Corner, 2001). Data gathered in focus groups under the specific sections of the model was used to recreate it under specific to this research circumstances, thus this is how the data would fill in the model, based on the two examples of behaviour (1) one which might be considered acceptable sometimes or mild online bullying whilst (2) the other would be considered unacceptable or online harassment):

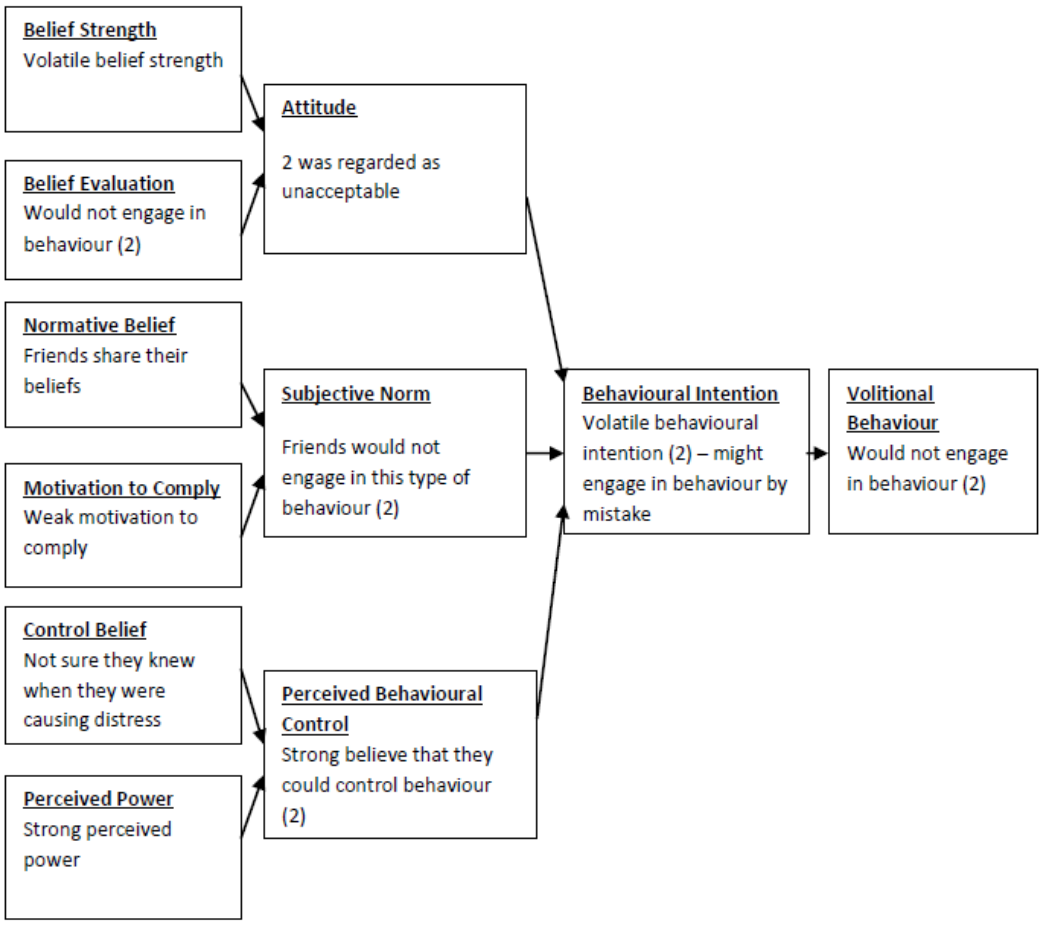


Figure 7. Theory of Planned Behavior (Ajzen and Fishbein's 1980) adapted.

It is crucial that we mention that this particular research piece does not test the model for online unacceptable behaviour but tries to speculate its effectiveness. Furthermore, we suspect the model might not work as well for online behaviour as so many of the premises of the model would not apply in virtual interactions and online behaviour.

Thus, starting from the premises that online interactions are different from real life interactions and that motives of engaging in unacceptable online behaviour might be different to motives for engaging in aggressive face-to-face behaviour, it was interesting to see what is the normative explanation as to why do students engage in unacceptable online behaviour. Focus group data reveals one very interesting finding: most participants (of which all the female) were convinced that some of the people experiencing cyberharassment or cyberbullying, deserve it because they themselves seek attention of that sort. This was argued as being a fact and the fact that young people post argument provoking posts and pictures of themselves online can only mean that they are also prepared to confront the nasty comments they might receive so they deserve it. Nevertheless, the same participants and especially the female participants strongly believed that women are more vulnerable than men, in the online environment. This finding is consistent with previous findings of Short and McMurray (2009) and Rivers and Noret (2010) which studied malicious communication via text messages and email and revealed that females went through a higher number of distressing experiences than men, thus it is safe to presume they are more vulnerable. Moreover, amongst normative beliefs on reasons of unacceptable online behaviour, participants thought it is also a matter of culture, social-background and generally individual differences. At the other end of the spectrum, another interesting finding on explaining why young people engage in unacceptable behaviour was revealed. Almost unanimously, participants of the focus groups came to the conclusion that their generation does

not take the online environment too seriously, that they often post things without thinking them through or assessing the impact it will have once it is out there. Of course, this underlines the grounds of Sulen's (2003) work in online disinhibition as people might act more impulsively when there is little real contact and said things they would normally not have said. Also, the fact that all of the student participants agreed they are not so much aware of what they are posting at all times and more so, they could not assess whether their posts or online actions are causing someone distress, only brings further evidence to the fact that their belief strength and control belief are weak and volatile. Furthermore, quantitative data reveals that people who consider unacceptable behaviour as being acceptable are people who scored higher on social comfort. This finding is consistent with findings from a Davies, Fleet and Besser (2002) study on problematic internet use. Their results show that people whose internet use is problematic are likely to score high on one of four dimensions, one of which is social comfort. Judging by implicit evidence, some of the focus group participants, which were more inclined towards seeing unacceptable behaviour as acceptable, will have scored higher on social comfort too.

The World Wide Web emerges as a chaotic world with few rules, most of them being technical and very little guidelines on behaviour so what norms do its users follow? Data from focus groups strongly suggests that to digital natives, online norms equal common sense. When asked what online norms they follow or when the context was related to this, virtually all participants said that to them, online norms are common sense, more specifically, if you would not do something in the 'real world' you will not do it online either, this includes all forms of aggression and unacceptable behaviour. Nevertheless, this created a paradox with the above mentioned perception that some people seek for negative attention online and like to stir controversy. In trying to explain this, focus groups reached the

conclusion that even though some people might be looking for attention, most often they do not expect negative reactions and mostly they are just looking for acceptance. Though when in some cases people cause harm knowingly and willingly, this was thought to be a personality trait and argued that probably those individuals are behaving unsocially outside the online environment too just that by having the online as a tool, and experiencing the disinhibitor factors mentioned by Suler (2003) they are more prone to acting aggressively online than offline.

8. CONCLUSIONS

This study manages to answer some of the most ardent questions in relation to the cyber space: Why do people engage in unacceptable online behaviour and what influences their behaviour? Does policy influence behaviour or act as a deterrent? What norms do young people follow when online? We managed to establish that there is no particular reason why people engage in unacceptable behaviour and sometimes behaviour becomes unacceptable by force of circumstances. Furthermore, policy on internet usage does not particularly influence students' online behaviour, nor they see this as a deterrent. Lastly, it seems that young people are learning though consequences of their own behaviour, sometimes painful rather than learning examples.

Talcot Parsons of the functionalist school believed that norms dictate the interactions of people in all social encounters. So if online interactions are thought to be social, what are the norms that people engaging in online behaviour follow? We presume it is safe to say that there is no set of written rules on how one ought to behave in a virtual environment. By definition, norms are informal and unwritten and usually people learn from each other, more specifically, generations learn from previous generations what is socially accepted. But the digital Era has

completely shifted this paradigm: young people became the ones using it (the internet) preponderantly before adults did and this is still the case today. So then, if there are no experienced adults guiding young people and acting as role models in this new world that they seem to own and run, who dictates the norms and based on what?

9. LIMITATIONS OF CURRENT RESEARCH

In terms of limitations of the current study we should acknowledge that whilst considered to be representative, the sample might lack in cultural and social representation as most of the questionnaire and all focus group participants are from Luton and belong to the University of Bedfordshire: so almost all normative beliefs are specific to this institution. Secondly, the questionnaire responses are possibly preponderant to the Computer Science and Technology department, which might have influenced quantitative results especially in terms of online skills. Thirdly, the focus groups were overseen by a member of staff, which might have partially inhibited respondents. Lastly, we admit that the response rate for the questionnaire was low and more respondents would have provided a better impression of the online behaviour. Furthermore, another notable limitation of this study is the time limitation. All research having been conducted at the same point in time, it only snapshots sample beliefs at that particular point in time. Another limitation of the study, independent from the researcher's capabilities, is the lack of up to date research in this area. Even though or perhaps because this area is so novel there is a paucity of research on the general subject of cyberstalking in the HE environment in the United Kingdom. More so, the researcher could not identify any piece of published work which would analyse behaviour in light of awareness of the AIUP (in HE environments). This is one of the downsides of the current paper as there is no precedent of similar research, the investigation process was

harder and possibly poorer than if there would have been reference points. Another impediment to conducting a more comprehensive piece of research was the fact that none of the universities contacted, in light of aiding this process by allowing access to their students and facilities, were responsive. None of the 12 universities contacted on numerous occasions were responsive.

10. RECOMMENDATIONS FOR FURTHER RESEARCH

Taking into consideration all of the limitation of this study, a direction for further research should be a more comprehensive, similar study, which could unfold over a longer period of time so as it would evaluate beliefs over a longer period of time. Furthermore, it would be interesting to note how beliefs change in time and what factors contribute to this. Provided that a similar study was conducted, on a larger sample, with a better cultural and social sample mix, it would be fascinating to understand all of the reasons for which people engage in unacceptable online behaviour (or at least analyse normative beliefs). Another direction for further research could constitute a study on the academic and non academic staff of HE institutions, with respect to AIUPs.

11. REFERENCES

Alexey, E. M., Burgess, A. W., Baker T., & Smoyak, S. (2005) ''Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention*, 5, pp. 279-289

Anderson, C.A., & Bushman, B.J. (2002) 'Human aggression', *Annual Review of Psychology,* (53), pp.27-51.

Anderson, J.Q., Boyles, J.L., Rainie, L. & Pew Internet & American, Life Project (2012) *The Future Impact of the Internet on Higher Education: Experts Expect More Efficient Collaborative Environments and New Grading Schemes; They Worry about Massive Online Courses, the Shift Away from On-Campus Life.* Pew Internet & American Life Project.

Armitage, C.J. & Conner, M. (2001) 'Efficacy of the theory of planned behaviour: A meta-analytic review', *The British Journal of Social Psychology / the British Psychological Society,* 40 pp.471-499.

Ajzen, I., & Fishbein, M. (1980) 'Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Baumgartner, S.E., Valkenburg, P.M. & Peter, J. (2010) 'Assessing causality in the relationship between adolescents' risky sexual online behavior and their perceptions of this behavior', *Journal of Youth & Adolescence,* 39 (10), pp.1226-1239.

Bradbard, D.A., Peters, C. & Caneva, Y. *Web accessibility policies at land-grant universities.*

Bullen, M., Morgan, T. & Belfer, K. & Qayyum, A. (2008) "The digital learner at BCIT and implications for an e-strategy.", *Research Workshop of the European Distance Education Network (EDEN) "Researching and Promoting Access to Education and Training: The Role of Distance Education and e-Learning in Technology Enhanced Environments"*, Paris, France October 20-22.

Consortium for, S.N. (2011) *Acceptable Use Policies in a Web 2.0 & Mobile Era: A Guide for School Districts. Consortium for School Networking*.

Day, K. & Schrum, L. (1995) 'The internet and acceptable use policies: What schools need to know', *The ERIC Review,* 4 (1), pp.9-11.

DeWall, C.N., Anderson, C.A. & Bushman, B.J. (2011) 'The general aggression model: Theoretical extensions to violence', *Psychology of Violence,* 1 (3), pp.245-258.

Douglas, K.M. & Sutton, R.M. (2010) 'By their words ye shall know them: Language abstraction and the likeability of describers', *European Journal of Social Psychology,* 40 (2), pp.366-374.

Eagly, A.H. & Chaiken, S. (1998) *'Attitude structure and function'*, in Gilbert, D. T., Fiske, S. T.& Lindzey, G. (eds.) *The handbook of social psychology, vols. 1 and 2.* 4th edn. New York, NY, US: McGraw-Hill. pp. 269-322.

Eagly, A.H. & Steffen, V.J. (1998) 'Gender and aggressive behavior; A meta-analytic review of the social psychological literature.', *Psychological Bulletin,* (100), pp.309.

Finn, J. (2004) 'A survey of online harassment at a University campus', *Journal of Interpersonal Violence,* 19 (468), pp.468-480.

Finn, J. & Banach, M. (2000) 'Victimization online: The downside of seeking human services for women on the internet', *Cyberpsychology & Behavior,* 3 (5), pp.785-797.

Finn, J. (2004) 'A survey of online harassment at a university campus', *Journal of Interpersonal Violence,* 19 (4), pp.468-483.

Flowers, B.F. & Rakes, G.C. (2000) 'Analyses of acceptable use policies regarding the internet in selected K-12 schools',*Journal of Research on Computing in Education,* 32 (3), pp.351.

Freis, S.D. & Gurung, R.A.R. (2013) 'A Facebook analysis of helping behavior in online bullying', *Psychology of Popular Media Culture,* 2 (1), pp.11-19.

Fremouw, W.J., Westrup, D. & Pennypacker, J. (1997) 'Stalking on campus: The prevalence and strategies for coping with stalking', *Journal of Forensic Science,* 42 (4), pp.666-669.

Gaskin, J.E. (1998) 'Internet acceptable usage policies', *Information Systems Management,* 15 (2), pp.20.

Gaskin, J.E. (1998) 'Internet acceptable usage policies', *Information Systems Management,* 15 (2), pp.20.

Gummesson, E. (2003) 'All research is interpretive!', *Journal of Business & Industrial Marketing,* 18 (6), pp.482-492.

Hare, R.D. (1996) 'Psychopathy: A clinical construct whose time has come', *Criminal Justice and Behavior,* (23), pp.25-54.

Howard, P.E., Rainie, L. & Jones, S. (2001) 'Days and nights on the internet - the impact of a diffusing technology', *American Behavioral Scientist,* 45 (3), pp.383-404.

Jung, J.Q., QIU, J.L. & Kim, Y.C. (1990) 'Comparative fix indexes in structural models', *Psychological Bulletin,* 107 (7), pp.238-246.

Lac, A., Crano, W.D., Berger, D.E. & Alvaro, E.M. (2013) 'Attachment theory and theory of planned behavior: An integrative model predicting underage drinking', *Developmental Psychology,* 49 (8), pp.1579-1590.

Lapidot-Lefler, N. & Barak, A. (2012) 'Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition', *Computers in Human Behavior,* (2), pp.434.

Lwin, M.O., Li, B. & Ang, R.P. 'Stop bugging me: An examination of adolescents' protection behavior against online harassment', *Journal of Adolescence,* 35 pp.31-41.

Maple, C., Short, E. & Brown, A. (2011) *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey.* University of Bedfordshire.

Margaryan, A.(.1.)., Littlejohn, A.(.1.). & Vojt, G.(.2.). (2011) 'Are digital natives a myth or reality? university students' use of digital technologies', *Computers and Education,* 56 (2), pp.429-440.

McNamara, C., L. & Marsil, D., F. (2012) 'The prevalence of stalking among college students: The disparity between researcher- and self-identified victimization', *Journal of American College Health,* 60 (2), pp.168-174.

Miller, L. (2012) 'Stalking: Patterns, motives, and intervention strategies', *Aggression and Violent Behavior,* 17 (6), pp.495-506.

Mogus, A.M., Djurdjevic, I. & Suvak, N. (2012) 'The impact of student activity in a virtual learning environment on their final mark', *Active Learning in Higher Education,* 13 (3), pp.177-189.

Neil, D., Leonidas, A. & Heather, F. (2009) 'The information security policy unpacked: A critical study of the content of university policies', *International Journal of Information Management,* (29), pp.449-457.

Ng, W. (2012) 'Can we teach digital natives digital literacy?', *Computers & Education,* 59 (3), pp.1065-1078.

Ogden, J. (2004) *Health psychology: A textbook 3rd edition.* England: Open University Press.

Pathé, M. T., Mullen, P. E., & Purcell, R. (2000). Same-gender stalking. Journal of the American *Academy of Psychiatry and the Law, 28, 191–197*.

Parsons-Pollard, N. & Moriarty, L.J. (2009) 'Cyberstalking: Utilizing what we do know', *Victims & Offenders,* 4 (4), pp.435-441.

Peng, T.Q. & Zhu, J. (2011) *Sophistication of internet usage (SIU) and its attitudinal antecedents: An empirical study in Hong Kong.*

Piotrowski, C. & Lathrop, P.J. (2012) 'Cyberstalking and college-age students: A bibliometric analysis across scholarly databases', *College Student Journal,* 46 (3), pp.533-536.

Schwarzer, R. (1992) *Self efficacy in the adoption and maintenance of health behaviors : Theoretical approaches and a new model , in R. Schwarzer (ed.), self efficacy: Thought control of action.* Washington,: DC Hemisphere.

Siau, K., Nah, F.F. & Teng, L. (2002) 'Acceptable internet use policy', *Communications of the ACM,* 45 (1), pp.75-79.

Spitzberg, B.H. & Hoobler, G. (2002) 'Cyberstalking and the technologies of interpersonal terrorism', *New Media & Society,* 4 (1), pp.71-92.

van Deursen, A. & van Dijk, J. (2009) 'Using the internet: Skill related problems in users' online behavior', *Interacting with Computers,* 21 (5-6), pp.393-402.

Suler, J. (2005) 'The online disinhibition effect'. International Journal of Applied Psychoanalytic Studies, 2 (2)

WANG, J., Chun-Fu C. Lin, Wei-Chieh W. Yu & &, E.W. (2013) 'Meaningful engagement in Facebook learning environments: Merging social and academic lives', *Turkish Online Journal of Distance Education (TOJDE)*, 14 (1), pp.302-322.