# "Cybercrimes in Educational Institutions: Understanding Student Vulnerability and Digital Misconduct"

**Sefoko Ramoshaba***

**Student Life and Development, Nelson Mandela University, Republic of South Africa**

**DOI: https://doi.org/10.47772/IJRISS.2026.100500102**

**Received: 29 April 2026; Accepted: 04 May 2026; Published: 23 May 2026**

## ABSTRACT

The advent and the rapid advancement of information and communication technology (ICT) has given rise to the complex matter of cybercrimes at educational institutions. The case of cybercrime emanates from the traditional crimes which are committed online like cyberstalking, cyberbullying, unauthorised sexting, sextortion, copyright infringements, piracy, access to of unauthorized data, online child pornography, swindling other students, ad infinitum. This study examines multifaceted role of ICT in igniting these cybercrimes. The study will look at the ICT technologies as the enabling instruments for cybercrimes. The anonymity of committing these cybercrimes amplifies the severity of these cybercrimes which may lead to significant repercussions to the cybervictims' psychological state and their academic performance. This study will also examine the ICT vectors used by perpetrators to commit these cybercrimes that include social medial platforms, messaging softwares and their applications, universities own internal ICT gadgets, softwares and educational platforms. The study will also look at the challenges faced by educational institutions in detecting, preventing, and managing these cybercrimes. The management of these cybercrimes must be done in a proactive manner than re-active manner. The study will argue that human centred and technological efforts are needed to curb the scourge of heinous cybercrimes.

**Keywords:** Cybercrime, Cyberstalking, Cyberbullying

### Research method

The qualitative research method was employed for this study, primarily through the application of systematic literature review as well as secondary data analysis. The secondary data were collected and assessed to examine cybercrimes educational institutions. The study used google scholar, ProQuest, ISI and ResearchGate to access articles or journals, online newspaper publications were sourced through google search engine, library journals and books received through the assistance of Nelson Mandela University Librarians. The search done through using words like cybercrimes, online bullying, online stalking, case studies of online crimes, methods of preventing and managing online crimes.

## INTRODUCTION

### Cybercrimes

Cybercrimes happen in the cyberspace or cyberworld. It is the newest concept emanating from the introduction of information and communication and its associated devices. Cybercrimes can have very serious consequences like loss of valuable and private data, and loss of lot of money. It manifests in various way including, hacking of social media accounts by fraudsters, online drug trafficking, software piracy, online computer fraud, continuous sending of undesirable or unwelcome messages, spreading rumours, terrorizing victims, identity theft, online fake recruitment schemes, online money laundering, intimidation, harassment, online extortion, intellectual infringement or fraud, critical damage institutions.

Cybercriminals utilize information technology and communication gadgets in their crimes against people, the state, and institutions. The well-known group of cybercriminals are black hat hackers, cyberbullies, cyberstalkers, impersonators, phishers, malicious information distributors, fake recruitment agencies, harassers,

flammers, cyber terrorists and online scammers. The literature indicates that there are minimal female stalkers than males. It is also argued that a significant number of stalkers have a criminal history of illegal substance abuse (Ahmed 2019: 7-13).

Students and young people are embracing the ICT revolution for their studying, interaction, online gaming and or meeting new acquintances. The problem is that there are henious individuals online who just want to harm or hurt other users. The mostly identified crimes are cyberstalking, cyberbullying, cyberharrassment, online pornography, identity theft, illegal online surveillance, spamming and hate speech. It is estimated that close to 500,000 young people above the age of 18 in the USA have been victims of these kinds of crimes (Alismaiel 2023: 1).

The table below indicate various forms of cybercrimes.

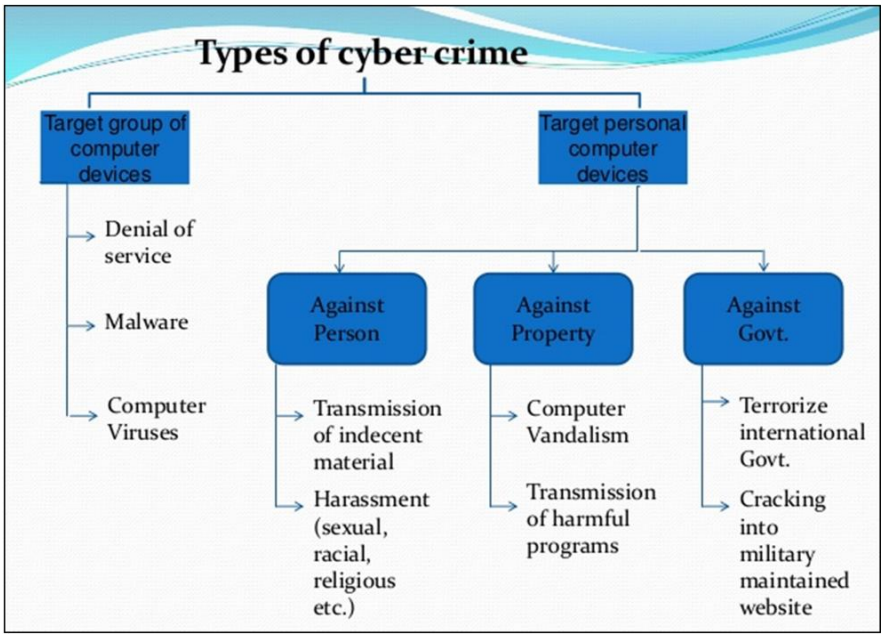


**Table 1: Telecommunication Development Sector: 2012. Types of cybercrimes: Understanding cybercrimes.**

These challenges necessitate proactive confrontation, as discussed next.

## Cyberbullying

Bullying is explained as intentional, repetitive, and harmful behaviour which is committed in an aggressive and manipulative manner against another person. It can be committed by one or more than one person against another person or a group of people (Reddy 2023: 1-7 & Sullivan 2011: 10-71). Bullying has moved to the online space since the advent of ICT revolution and its continuous advancement, and it is conducted in an electronic or online format. More than half of the citizens of the USA who are online might have experienced cyberbullying (Arif, Qadir, Martins and Khujwala 2024: 1-16).

There are disadvantages of using information technology devices, as one may encounter cyberbullying or internet aggression which relates to a form of online harassment. There is sexual harassment where unfavourable sexual comments or request for sexual favours are involved. This has caused grave forparents as this has been identified as one of the main problems with social networking sites and instant messaging services. Cyberbullying refers to various forms of unwanted aggressive behaviour on the internet which may sometimes involve the threat of violence. It relates to the use of information technology and its associated devices or electronic equipments to commit bullying. These information technology devices may include one or more of the following: Cell phones; Web sites; Blog sites; emails, computers, pagers, and internet voting websites. These technological devices are used to threaten or intimidate other people with violence or harass them continuously with inhumane or harmful conduct by one person or a group of people towards another person or a group of people, with the aim of hurting them. The main characteristics of these conduct is that it is continuous, intentional

and harmful. This can be regarded as a virtual and cruel social crimes. Cyberbullying has increased at educational institutions the increasing availability of electronic devices. All ages, male and female, are involved in cyberbullying, Females who frequently use the internet are likely to be bullied than males (Swearer, Espelage & Napolitan 2009: 109-118).

Students who commit cyberbullying usually have their own justifications for committing it. These reasons range from jealousy, paying revenge for oneself or friends; wanting to be in charge or feeling that they are powerful to do anything; seeing it as a joke or a funny exercise; a ploy to keep loneliness away; personal satisfaction when bullying someone; the desire to harm others; failure to understand the seriousness of cybebullying and its impact. They believing that it is fine to bully others and the desire to simply exhibit aggressive behaviour (Trolley & Hanel 2010: 31-47).

Cyberbullying can be committed by a person known by the victim or a stranger who just exists on the cyberspace. There has been a rise in the incidences of cyberbullying even though some cases may not have been reported to parents or authorities. Many students had agreed that they have been bullied and it is a bad experience, even though they did not report it. The lack of reporting may deny researchers accurate data of the occurrence of. cyberbullying.

**Manifestations of Cyberbullying**

Cyberbullying manifests itself in various ways and below are some of the ways:

1. Students may start cyberwars by sending each other hateful and vulgar messages (flaming).

2. Students send provocative, offensive and vulgar messages in a continuous manner (harassment).

3. Students engage in online activities that result in another student feeling terrified and under threat of his or her surroundings. This kind is normally referred to as cyberstalking.

4. Students posting malicious rumours about other students online which damages their good character and personal relationships. This is referred to as denigration.

5. Students creating a fake web site where they pretend to be a fellow student and proceed to post dangerous or bad messages which make the other student look and feel bad. It also attacks the person's social standing and relationships with other people and it is referred to as impersonification.

6. Students distributea fellow student's personal or private life in order to embarrass or humiliate them on electronic chat sites. This may include posting embarassing pictures of that particular person and is referred to as outing.

Students may deliberately cause their fellow student share her or his private life with them which they will latter share with whole world online. It is done in order to hurt or harm a fellow student. It is just a trickery (Reddy 2023: 5-6 & Trolley & Hanel 2010: 31-47).

**Cyberbullying: Signs of Victimization**

There are indicators that indicate if a particular student has been bullied or has bullied others. Parents and authorities need to take note of them (Trolley & Hanel 2010: 31-47).

Indications of a student who has been a victim of cyberbullying are: annoyance after using electronic devices, does not like topics on proper usage of electronic devices, nervousness upon receipt of emails or text messages, bad mood swings; stops utilizing electronic devices, suicidal tendencies, eating disorders, depression, other chronic illnesses, social exclusion, running away from home, and responding with acts of violence or engaging in criminal activities, they stop socializing, poor academic performance at school, and nervousness or anxiety when meeting friends (Reddy 2023: 5-7 & Trolley & Hanel 2010: 31-47). The above indicators are not all inclusive.

**Britain's Cyberbullying Study**

Cyberbullying is like normal or general bullying that has moved to the cyberspace because of the advent of information and technology revolution. Its impact is sometimes like an online war. The beatbullying study in Britain indicated that one in thirteen children had been bullied one way or the other using information technology gadgets and or devices. It is a daily occurrence, and it may be perpetrated by a single individual, or a group of individuals. The continuous bullying may last for more than twelve months for one individual being cyberbullied by the same person or group. The impact of cyberbullying is like those of physical face to face bullying. It results in painful impact on the lives of victims. There are victims who had killed themselves after relentless bullying on social networking websites like Bebo and Facebook. Victims may feel isolated, they perform badly at school because of this distraction. The victims may also delve into self-destructive behaviour.

Cyberbullying may also manifest itself through sexting. Sexting relates to the texting of sexually explicit images, nude images, or sexual suggestive actions amongst themselves. It may sometimes manifest itself in a bad sexual language or unwanted sexual language.

It is said that females are more likely to be exposed to bullying: two times more than boys. Fourty-eight percent of male victims had agreed to have bullied someone. Many videos of bullying has been posted on You Tube, Bebo and MSN instant messenger services.

This kind of behaviour is a menance to the society and strategies of managing it has eluded authorities for far too long. The British government, in its bid to stop cyberbullying, has produced certain measures. Beatbullying is one of the websites that have been developed to assist victims of cyberbullying in Britain. They have also developed programmes like cybementors', deisgned to help victims of cyberbullying. It is a peer monitoring programme which can be accessed via social networking sites. It helps children who experienced bullying online. Peer groups provide assistance to the victims of online bullying who understand and know what bullying is. They minimise the stigma associated with the fear of speaking about bullying or being a victim of bullying. The programme gives the victims of bullying the energy of putting bullying away from their way (Paine 2009: 161).

**The Crime of Sexting, Sextortion and Doxing**

Sexting like cyberbullying and cyberstalking are legally deemed to be criminal misdemeanours and punishable in courts of law. Cyberbullying and cyberstalking can both be connected to sexting abuse. *Sexting* abuse is the sending of sexually graphic photos to other people other than a victim with the aim of hurting and embarrassing the victim. The photos are normally nude and sexually graphic photos which the victim may have previously shared with the bully with whom they are no longer in love. They are sent to a huge number of people online through social media platforms, emails, cellphone messages and other existing forms of electronic messaging systems. Sometimes the photos are sent to the families of the victims like parents, siblings, aunts, uncles, and close family members. They may also be sent to a certain group of people who are close to the victim like school mates or classmates. The impact of sexting may last forever on the victim which may to mental health and possibly suicide.

Recent research studies on sexting have showed that when girls refuse to provide new photos to the perpetrator, the perpetrator will use the old photos that were sent to him or her to cyberbully or extort the victim to send more new nude photos. Boys can also be victims of sexting; it is not gender specific. It is harassment or ask a victim to provide more sexually graphic photos (Duke 2021: 1-3).

There are many instances where it has been discovered that tthe widely distributed photos, images and or videos of a victim are not even real or original. They have been manipulated through the information and communication technologies like software to create the fake photos that looks real or original. These fake images, messages, voices, and photos will be widely distributed on existing online platforms like social media, email, cellphones, computers, laptops, and other forms of electronic websites. The aim is to commit an act of sexting the victim to harm or hurt and embarrass or shame the victim (Maras & Logie 2024: 1).

This new trend of sexting is regarded as synonymous to revenge pornography. It is a non-consensual pornography distributed all over websites and social media platforms without the knowledge of the owner of the photos, videos, or images. It is normally conducted by a bully who might have been in sexual relationship with the cyberbullies or cyberstalkers when the love ends. It is getting famous just like sexting with the same connotations and desired end results. Research indicates there is close to two thousand fuckme kind of revenge porn websites globally. Victims have been hurt, dignity impugned, dehumanised, embarrassed, been caused emotional and mental distress, and humiliated around the globe by their sexual and intimate images, photos, voices, and videos being wildly displayed in different online platforms. Strict laws, guidelines, and policies to combat the scourge of heinous and unspeakable, disgusting, awful act of sextortion and sexting. Offenders or perpetrators must be punished with seriousness it deserves, whether through parents, the judiciary, and educational institutions. Their local communities must shun them (Hinduja 2025: 1-2 & Legal Wise 2025: 1-2).

One girl from USA in Ohio committed suicide after her sexually explicit pictures/naked breast were circulated to her school mates by her former boyfriend. The former boyfriend received a jail sentence (Chetty 2009: 1-2).

**Cyberstalking Prevention Strategies**

Cyberstalking is sometimes regarded as a crime of cyberbulling in the literal sense (Reddy 2023: 6). The literature indicates that there are minimal female stalkers than males. It is also argued that most or some stalkers have a history of criminal offences of illegal substance abuse. The most common victims of cyberstalking are females than males and cyberstalking is closely related to Gender-Based Violence (Ahmed 2019: 40-41 & 48).

The online crime of cyberstalking and its impact on the victims is profoundly serious and devastating. Cyberstalking is regarded as the harassment, intimidation or threatening of other people using information technology and its associated devices. The information technology devices may include one of the following: internet, pagers, Facebook, twitter, cellphones, YouTube, and emails. These information technology devices make cyberstalking an easier phenomenon because of its anonymity. It is mostly directed towards women aged between 18-24. They have been on the receiving end of serious offences like cyberstalking and sexual harassment (Ahmed 2019: IV).

In 1999, Al Gore, the former Vice President of the USA has indicated that cyberstalking is another form of gender-based violence which sees women harassed, and intimidated (Ellison 2001: 1).

Cyberstalkers can also use third party cyberstalkers to help them stalk their victims using electronic devices. Cyberstalkers can also create websites where they attack their victim and invite other people to continue with the cyberstalking. Internet chat rooms, blogging sites and newsroom are also used to stalk people.

In recent times, the level of cyberstalking has increased, and the number of victims is unknown as even though many people have reported that they have been cyberstalked (Maxwel 2001: 1-28 & Nurse, Jason, and Budi 2020: 6-10), several others do not report when they are cyberstalked.

Adam Maxwell Donn who resides in Virginia (Norfolk) was sentenced to fifteen months for stalking and fined an amount $2 380 to the victim of cyberstalking. The sentence has been added with extra supervision for the three …???? when he is out of jail. He was sentence by Judge Eagan. He was stalking G.T. Bynum who is the former mayor of Tulsa, and his family was also cyberstalked (U.S. Attorney's Office, Northern District of Oklahoma 2021: 1).

There are better and responsible ways in which students and young people can utilize information technology and its associate devices and or gadgets. The following guidelines can assist in managing online wars or bullying by young people:

1. A person must treat others the way they would also like to be treated.
2. Speak with people using a proper and respectful language.
3. Professionalism in what you write and how you write it is crucial.

4. Avoid offensive and discriminatory messages.
5. Avoid circulating people's confidential information or personal details in public.
6. Avoid reading people's messages without authorization.
7. Avoid publishing your employer's privileged information like trade secrets.
8. Make sure you send your messages to the right people.
9. Always respect your or institutions' policy on responsible usage of internet.
10. Always keep your access code private.
11. Do not use other people's access secret codes without permission.
12. Never get involved with messages or images that discriminate other people.
13. Never get involved with messages that sexual assault children.
14. Never promote hatred on the internet.
15. Do not harass people on the internet.
16. Do not attack people on the internet.
17. Do not get involved with malicious messages on the internet.
18. Do not get involved with computer swindlers or fraudsters.
19. Never post dangerous information like how to make explosives.
20. Never post incorrect information on the internet.
21. Never give out your personal details to strangers on the internet.
22. Treat cyberspaces love affairs carefully before you get hurt.
23. Be on the lookout for internet swindles like people requesting your credit card number.
24. Always credit when using internet sources.
25. Respect copyright legislation when using internet.
26. People must know their rights when using internet, like the right to privacy and the right not to be harassed.
27. People have a right not to receive pornographic messages or images (Willard 1997: 1-101 & Zong, Qui, Sun, Jin, Zwang, Guo, Jin, Guo, Xu, Huang & Zheng 2022: 1-16).

The educational institutions must use the above-mentioned guidelines to design ICT codes of conduct that will provide guidance to learners and students on the ethical behaviour that is acceptable withing the institutions. The codes of conduct must also indicate the unethical behaviour that is unacceptable and the types of punishment that will be meted against the offenders. Section 8 below assist in providing the methods that can used by institutions to curb the scoured of the heinous cybercrimes.

**Methods of Preventing the Cybercrimes**

There are better methods of preventing the abuse of information technology and associated devices by students and young people in general. Institutions mustschools must design codes of conduct that encompases the responsible usage of electronic communication devices. Parents' involvement in the management of the responsible usage of information technology and associated devices is key. Proactive methods of managing cyberbullying are needed. The parents must make rules at home on the proper usage of computers and its associated devices. These rules may as follows:

1. Computers must be placed in an open area for proper supervision;
2. There must be time limitations for children when it comes to computer usage;
3. Explain what a child may view or not view on the computers;
4. Children must be warned against providing private and personal information to strangers;
5. No pornographic pictures or video clips;
6. Teach children how to deal with online bullies;
7. Children must not give away their internet passwords to anyone;
8. Children must know that there is a consequence for every action they take online;
9. Children must be taught how to use computers responsibly;
10. Children must learn to stop using computers when bullied;
11. Children must store all evidences of bullying when bullied;
12. They may also store this information with other people they trust.

Learnes and students must be taught conflict resolution skills in order to deal with bullies online. Social interaction skills must be instilled on them from an early stage. Development programmes are necessary in order to prepare them in managing cyberbullying. Psychologists, social workers and students development practitioners must be responsible for developing learners and students' character to be responsible citizens (Bailey 2008: 10, Ramoshaba 2017:71 & Trolley & Hanel 2010: 77-82).

**The Painful Experiences of Cyberbullying**

Cyberbullying has been seen to be prevalent amongst young adolescent in Thailand schools than primary schools. The adolescent cyber-harass and cyber-victimize each other online than any other groups of young people (Suraseth & Koraneekij 2024: 1-16).

This section outlines students' bad and painful experiences of cyberbullying, which is sometimes committed underground where it is not visible to a bystander or a neighbour. Hundred and thirty-one social science, technology and education undergraduate students were interviewed with a survey questionnaire. Seventy-three were females and fifty-seven were males. The questionnaire had twenty-seven items related to cyberbullying. Fifty-four percent of the respondents and hundred percent of male respondents indicated that they know a person who had been once cyberbullied. The cyberbullies had used cellphones, Facebook, and instant messaging services. The study has outlined the rate of cyberbullying on undergraduate students at universities. It had focused on both victims and perpetrators. It is also said that bullying may either be direct or indirect.

There is an extension from a student being a perpetrator of bullying from pre-school, primary, secondary, high school and at university levels. This situation is also applicable to the victims. The impact of bullying may lead to suicidal thoughts, depression, and uneasiness with nervous breakdown. It may also result in alcohol abuse,

mental problems, and poor academic performance. Section 10 below indicates the different manifestations of cyberbullying.

**Distinct Types of Cyberbullying Cases**

The table below indicates the type of cyberbullying acts students have been exposed to.

**Table 2. Types of cyberbulling acts.**

| Item | Description | N | % |
|---|---|---|---|
| A | Sending tokens of affection (e.g. poetry, songs, electronic greetings, praises, etc.) | 40 | 33 |
| B | Sending exaggerated messages of affection (e.g. expression of affection implying a more intimate relationship than you have, etc.) | 33 | 28 |
| C | Sending excessively explicit messages (e.g. inappropriately giving private information about his/her life, body, family hobbies, sexual experiences, etc.) | 31 | 26 |
| D | Sending excessively 'needy' or demanding messages (e.g. pressuring to see you, assertively requesting you to go out on a date, arguing with you to give him/her 'another chance', etc.) | 36 | 30 |
| E | Sending pornographic/obscene images (e.g. photographs or cartoons of nude people, or people or animals engaging in sexual acts, etc.) | 28 | 23 |
| F | Sending threatening written messages (e.g. suggesting harming you, your property, family, or friends, etc.) | 15 | 13 |
| G | Sending sexually harassing messages (e.g. describing hypothetical sexual acts between you, making sexual demeaning remarks, etc.) | 14 | 12 |
| H | Sending threatening pictures or images (e.g. images of actual or implied mutilation, blood, dismemberment, property destruction, etc. | 3 | 3 |
| I | Exposing private information about you to others (e.g. sending email out to others regarding your secrets, embarrassing information, unlisted numbers, etc. | 14 | 12 |
| J | Pretending to be someone else he or she wasn't (e.g. falsifying representing him/herself as a different person or gender, claiming a false identity, status, position, pretending to be you, etc. | 14 | 34 |
| K | Sabotaging' your private reputation (e.g. spreading rumors about you, your relationships, or activities with friends, family, partner, etc.) | 19 | 16 |
| L | Sabotaging' your work/school reputation (e.g. spreading rumors about you, your relationships, or activities in organizational networks, electronic bulletin boards, etc. | 8 | 7 |
| M | 'Friended' people you know to get personal information about you | 37 | 31 |

Table 2: Types of cyberbulling act. Walker, Sockman, and Koehn 2011: 35

The table above clearly indicates that cyberbullying is real. Institutions must design strategies for dealing with cyberbullying, cyberbullies and helping victims of cyberbullying. It must be norm to always look at ways of protecting students from cyberbullies (Walker, Sockman & Koehn 2011: 31-38). Cybervictims of cyberbullying have the highest level of pain and or agony (Schneider, O'Donnell, Stueve, and Coulter 2012: 171-175).

**Practical Strategies of Managing Cyberbullying**

There are other ways of managing bullying and namely:

1. Online ethical behvaiour must be promoted.

2. Online or internet ethical digital natives must be enforced at all times.
3. learners and students must block or walk away from haters and online bullies;
4. Possible strategies of dealing with bullies, victims and witnesses of bullying must be designed and implemented.
5. Educators and administrators must receive training on how to manage bullying.
6. There is a need to monitor bullying at all times.
7. There is a need to constanlty amend bullying guidelines whenever there is a need in term of the legal framework outlined by the government;
8. There must various ways of promoting anti-bullying behaviour;
9. Rules must be enforced constantly and consistently.
10. Online anonymous reporting must be encouraged.
11. Police Services must be involved in serious cases.
12. Parents and the community must help in manmaging bullying.
13. Educators must be equipped with strategies of managing bullying in classes.
14. Pyschological referrals may also help in managing bullying at schools.
15. Cases of bullying must be attended to as soon as practically possible.
16. Bullies and victims must be interviewed separately if there is a case of bullying.
17. Bullies must be reminded about the code of conduct and possible sanctions;
18. The victim must know that the institution is on their side.
19. The authorities must teach and promote the code of conduct and the consequences of breaching the rules.
20. The bully's and the victim's parents must be informed as soon as possible if a case of bullying has been opened.
21. Victims must be constantly checked if they are still safe.
22. Victims must be encouraged to always talk to the educators and administrators if there are problems associated with bullying at school.
23. If the bully does not repent, he or she must be taken out of the institution..
24. Parents must monitor their children's social media accounts and cellphone activities;
25. Monitoring of the websites visited by learners and students.
26. Parents must know social media accounts of their children (Stopbullying.gov 2025: 1-20 & Vermont Department of Education 2004: 1-3). The section below will provide the findings of th this study.

**The South African Context of Cybercrimes**

Educational institutions are the fertile grounds for cybercrimes because of the nature of the university structure (many employees and students). They are characterized by a large base of existing banking details from students and employees. They have a lot of copyrighted information, publications and research information. This attracts cybercriminals into their fold who are ready to conduct their cyberattacks. Some institutions have resources to prevent and manage the cases of cybercrimes, but all of them have such abundance of resources. Some cybercriminals extort them by threaten to sell off the stolen information. The staff members of these institutions were offered training module on how to prevent and manage cybercrimes. The training was developed by the Training for Network Security Team Staff members (TRANSITS) around the globe. Some modules were tailor made for the South African context (TENET South Africa 20202: 1).

The Ipsos research has found out that South Africa has the highest rate of cyberbullying cases of young people in the whole world. South Africa had 51% of cyberbullying cases against the world average of 37%. The difficulty with managing cyberbullying cases is the anonymity provided using the internet-based ICT technologies and related devices. The perpetrator can use fake names or identity. It becomes difficult to know the identity of the cyberbully. A lot of cases were reported during the COVID-19 pandemic period. The cybercrime of hate speech was also worse during th Covid-19 pandemic amongst the teens. The cyberbullying study conducted by the Nelson Mandela University has discovered that 37% percent of the respondents have faced cyberbullying. One of the concerning points is that most respondents have indicated that they are not aware on how to deal with cyberbullying. The South African government has established various instruments to manage cybercrimes. The National Cybersecurity Policy Framework which contains methods of preventing cyberbullying and how victims can be protected. The Filma and Publications Board has been given a mandate to monitor and regulate the cyberspace content. The Board manages cybercrimes like cyberbullying and other internet-based crimes. The Cybercrimes and Cybersecurity Bill was introduced in 2018 by the parliament which criminalises cybercrimes. The frame allows educational institutions to come with guidelines of managing cybercrimes, promoted good ethical online citizenship. All these plans are done to create a more inclusive, safer, and ethical digital world (Masiphephe Network 2023: 1-3).

Thandi, one of the female students at the University of Cape Town (UCT) in South had experienced cyberstalking by her former lover called Dave. Dave photoshop ed Thandi's face on the nude body that he photoshop ed. It was displayed on Facebook. Thandi was devasted emotionally and psychologically, but she had a support of her friends. Dave will even stalk her physically like he would visit the same night clubs which she visited with her friends at the same time. Dave combined physical and cyberstalking against Thandi. Thandi ended up reporting Dave and he received a jail sentence for his behaviour (UCT 2025: 1-2).

These pictures may be displayed or be in any of the following forms: sexual contact, helping to participate or participating in a sexual act, sexual penetration, action that depict sexual offences, self-masturbation, images of sexual body parts, forcing a person to show his or her anus or sex organs, stimulation of a person's breasts, sexual suggestive images or lewd acts, committing sadistic acts with sexual connotations, engaged in an act of sexual intercourse and committing any sexually related act (Chetty 2009: 1-11). Apart from sextortion, there is also an abuse called doxing" where perpetrators publicize personal details of a victim in websites and social media platform asking people to help him or her to collect money owed by the victim Legal Wise (2025: 1-2).

Cyberbullying, sexting, and revenge pornography are the most common cases in South Africa. One of the South Africa's Digital Law Firm has indicated in 2024 alone, the firm has received lot of cases or complaints on the cybercrime of revenge porn, sextortion, and cyberbullying. This happened during the Covid-19 lockdown period. The law firm had advised victims to record all the postings of these cybercrimes which may or can be used as evidence at a later stage. The victim can report a case at the local police station and report the perpetrator to a specific social platform that was used to commit these heinous crimes (Farrel 2022: 10).

Miss Zanele Sifuba was entangled in the devasting cybercrime of revenge pornography by her former boyfriend who widely distributed sexually explicit videos and photo on social media. The boyfriend did this to her as part of his revenge while humiliating and harming her on the social public domains. The boyfriend received the videos based on trust because they were lovers once upon a time. The video was only meant for the benefit of

her lover without knowing that it will be used against her. This happened in 2023. The lady nicknamed the "Spar lady" was victimised by her former lover who distributed her sexually explicit or graphic video of her on social media as part of harming and humiliating. It needs to be noted that revenge pornography is not a victim's induvial predicament only. It is a societal problem of patriarchy, sexism, objectionism and gender-based violence against women. The victims face hurt, humiliation, their privacy is violated and abused (Magayana 2024: 1). In South Africa, there are laws that has been enacted to punish the perpetrators of the cybercrime of revenge pornography. The law is called the Film and Publications Amended Act 11 of 29. The act is designed to punish the people who illegally publish graphic sexually or nude videos and sex recorded tapes of other people or former lovers (Brook 2020: 1).

## THE FINDINGS

The literature review and the existing body of knowledge clearly indicate the dangers of cyberspace for learners and studens at educational institutions.eneral. Cyberstalking, cyberbullying, online sex crimes, cyber-harrasmmnet, identity theft, and other associated crimes exist. They are a danger for leaners and students.The study confirms that legislationn, police and courts and statutory bodies and policies and guidelines

It has been found out that cybermentors and or cyber peerhelpers need to be introduced They will assist in preventing and managing cybercrimes. They will orientate other learners and students on how to surf in a safer and vigilant manner from henious and unscrupulous criminals lurking online. The cbermentors story of Briatain can be transferred into the South African context where the mentors will be trained on how to guide the victims on how to repospond and the necessary steps need to be taken when reporting cybercrimes. They will also conduct awareness campaigns and training on the dangers of cybercrimes. They can also participate in the welcoming and orientation of irst year students.

The study also confirms that the victms of cyberbullying experiences emotional and pschological trauma. This trauma may lead to humiliation, trauma, anxiety, and depression that may lead to mental health challenges. South Africa has the legistalions and guidelines that dealing with cybercrimes but it continues unabated. These crime preventions methods and their punishement on the cybercriminilas must be implemented without or favour.

Finally, the study indicates that there is need to make concerted efforts in addressing and preventing all forms of online crimes from our educational institutions. Section 11 below deals with the conclusion and recommendations of this study of cybercrimes.

## CONCLUSIONS AND RECOMMENDATION

This study of cybercrimes indicates the vital need for educational institutions to treat the scourge of cybercrimes and its impact on the cybervictims with the seriousness it deserves. The study noted the emotional and psychological impact of cybercrimes on its victims. The impact may be anxiety, depression and trauma which may lead the students and leaners to feel like self-harming themselves and committing suicide because of depression. The impact may also be devasting on the students' success on their studies and deny them their right to education. Educational institutions must source robust cybersecurity instruments, conduct awareness campaigns on the dangers of cybercrimes and design policies and or guidelines that will assist in preventing and managing cybercrimes. Thes measures will assist in protecting the staff members and the study body. The measures taken against cybercrimes must also be able to protect the university ICT infrastructure and associated devices and or gadgets. They must also be able to identify and squash any potential threat to the ICT infrastructure. This will assist in enhancing the culture of learning and teaching.

This study explored the potential role of senior student cybermentors in preventing and managing cybercrimes. Cybermentors can play a vital part in promoting cybersecurity awareness, providing guidance, and supporting their peers in navigating online dangers and risks. Institutions must leverage cybermentors' tech-savviness and use it to to teach and promote cyberethics. They will foster the culture of cybersecurity, enhance digital literacy, and reduce cybercrime vulnerabilities. The four key performance areas for cybermentors may be the following or more, namely: awareness campaigns, peerhelp support to the student body, promotion of cybersecurity skills,

and teaching students what to do in case a student is a victim of cybercrime. The cybermentors can assist in creating the environment that is conducive for learning and teaching by preventing and managing cybercrimes efforts. The cybermentors must also play the role of Ethics Officers, who promote ethical behaviour within educational institutions. Educational institutions must strive to create a safe online world. They must enhance an environment that is conducive for learning and teaching, with no cybercrimes.

**Abbreviations**

| | |
|---|---|
| ICT | Information and Communication Technology |
| UCT | University of Cape Town |

**Author Contributions**

Sefoko Ramoshaba is the sole author. The author read and approved the final manuscript.

**Conflicts of Interest**

I hereby declare that I do not have vested interest in the content of this journal.

## REFERENCES

1. Ahmed, N. 2019. Cyberstalking: A Context Ananlysis Gender-Based Violence Offences Committed Online. University of KwaZulu Natal.
2. Alismaiel O.A. 2023. Digital Media Used in Education: The Influence on Cyberbullying Behaviors Among Youth Students. Int J Environ Res Public Health. 2023 Jan 12; 20(2): 1370. https://doi.org/10.3390/ijerph20021370. PMID: 36674128; PMCID: PMC9858636. (Accessed 23 March 2025).
3. Allison, E. 2001. Crime and the Internet. Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203299180-12/cyberstalking-louise-ellison (Accessed 13 March 2025).
4. Arif A, Qadir MA, Martins RS, Khuwaja HMA (2024) The Impact of Cyberbullying on Mental Health Outcomes Amongst University Students: A Systematic Review. https://doi.org/10.1371/journal.pmen.0000166 (Accessed 09 March 2025).
5. Bailey, D. 2008. Cyber Ethics. New York: Rosen Publishers.
6. Brook, M. 2024. South Africa Cracks Down on Revenge Porn. Schindlers. https://www.schindlers.co.za/south-africa-cracks-down-on-revenge-porn/ (Accessed 08 Mar h 2025).
7. Carol M. Walker, Beth Rajan Sockman and Steven Koehn. An Exploratory Study of Cyberbullying With Undergraduate University Students. TECHTRENDS TECH TRENDS 55, 31–38 (2011). https://doi.org/10.1007/s11528-011-0481-0 (Accessed 08 April 2025).
8. Chetty, I. 2009. Sexting-Child-Pornography. https://efaidnbmnnnibpcajpcglclefindmkaj/https://www.childlinesa.org.za/wp-content/uploads/sexting-child-pornography.pdf (Accessed 15 March 2025).
9. Duke, A.M. 2021. Advancing Bullying Awareness: Cyberbullying, Cyberstalking, Sexting & the Law. Extensions: Alabama A & M and Auburn Universities. https://www.aces.edu/blog/topics/home-family/advancing-bullying-awareness-cyberbullying-cyberstalking-sexting-the-law/ (Accessed 08 March 2025).
10. Farrel, J. 2022. What to Do if You are Targeted for Revenge Porn, Sextortion, and Cyberbullying. https://www.news24.com/life/what-to-do-if-you-are-targeted-for-revenge-porn-sextortion-and-cyberbullying-20220728 (Accessed 08 March 2025).
11. Hinduja, S. 2025. Revenge Porn Research, Laws, and Help for Victims. Stomp out Bullying. https://www.stompoutbullying.org/blog/revenge-porn-research-laws-and-help-victims (Accessed 11 March 2025).
12. Legal Wise. 2025. Online Abuse Women. it's on the Rise. https://www.legalwise.co.za/news/online-abuse-against-women-its-

rise#:~:text=Abuse%20against%20women%20is%20a,the%20use%20of%20social%20media. (Accessed 17 April 2025).
13. Magayana, S. 2024. Harsh Reality of Revenge Pornography: Time to Take a Stand Against it. University of Free State. https://www.ufs.ac.za/templates/news-archive/campus-news/2024/february/harsh-reality-of-revenge-pornography-time-to-take-a-stand-against-it (Accessed 10 March 2025).
14. Maras, H-M and Logie, K. 2024. Countering the Complex, Multifaceted Nature of Nude and Sexually Explicit Deepfakes: An Augean Task? A Journal of Crime Science. Vol.13(31): https://link.springer.com/article/10.1186/s40163-024-00226-6 (Accessed 11 March 2025).
15. Masiphephe Network 2023. The Impact of Cyberbullying in South Africa. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.masiphephe.org.za/wp-content/uploads/2023/05/3.-Thematic-paper-cyber-bullying-in-SA_FINAL.pdf (Accessed 11 March 2025).
16. Paine, T. 2009. Virtual Violence: Protecting Children From Cyberbullying. The Rights of Man. 1791(II): 1-61.
17. Ramoshaba, S. 2017. Improving the Management of Inappropriate Utilisation of Information Technology. University of Johannesburg. https://ujcontent.uj.ac.za/esploro/outputs/doctoral/Improving-the-management-of-inappropriate-utilisation/9912812207691 (Accessed 06 March 2025).
18. Reddy, S. 2023. Providing a Legal Definition for Cyberbullying in South Africa. Obiter Vol.44 No.4 Port Elizabeth 2023. Version On-line ISSN 2709-555Xversión Impresa ISSN 1682-5853. (Accessed 11 March 2025).
19. Schneider S.K, O'Donnell L, Stueve A, and Coulter R.W. 2012. Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students. Am J Public Health. 2012 Jan;102(1):171-7. doi: 10.2105/AJPH.2011.300308. Epub 2011 Nov 28. PMID: 22095343; PMCID: PMC3490574. (Accessed 14March 2025).
20. Stevens, Francesca, Nurse, Jason R. C. and Arief, Budi. 2020. Cyber Stalking, Cyber Harassment and Adult Mental Health: A Systematic Review. Cyberpsychology, Behavior, and Social Networking. ISSN 2152-2715. https://doi.org/10.1089/cyber.2020.0253 (Accessed 10 March 2025).
21. Stopbully.gov. 2025. How to Prevent Cyberbullying: A Guide for Parents, Caregivers, and Youth. https://efaidnbmnnnibpcajpcglclefindmkaj/https://www.stopbullying.gov/sites/default/files/documents/Cyberbullying%20Guide%20Final%20508.pdf (Accessed 15 April 2025).
22. Sullivan, K. 2011. The Anti-Bullying Handbook. 2nd Edition. London: Sage.
23. Schneider, S. K., O'Donnell, L., Stueve, A., & Coulter, R. W. S. (2012). Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students. American Journal of Public Health, 102, 171-177. https://doi.org/10.2105/AJPH.2011.300308 (Accessed 15 April 2025).
24. Suraseth C, Koraneekij P. Cyberbullying Among Secondary School Students: Analyzing Prediction and Relationship With Background, Social Status, and ICT Use. Heliyon. 2024 May 6;10(9):e30775. doi: 10.1016/j.heliyon.2024.e30775. PMID: 38756584; PMCID: PMC11096923. (Accessed 11 April 2025).
25. Sweaterer, S.M., Espelange, D.L., and Napolit, S.A. 2009. Bullying Prevention and Intervention: Realistic Strategies for Schools (The Guilford Practical Intervention in the Schools Series). 1st Edition. https://www.amazon.com/Bullying-Prevention-Intervention-Realistic-Strategies/dp/1606230212 (Accessed 15 March 2025).
26. Telecommunication Development Sector. 2012. Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU Telecommunication Bureau. http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html (Accessed 27 February 2025).
27. TENET South Africa. 2020. Responding to Cybercrime in South Africa's Higher Education and Research Community. https://www.tenet.ac.za/news/responding-to-cybercrime-in-sa-rne (Accessed 09 March 2025).
28. Trolley, B.C., and Hanel, C. 2010. Bullying in Secondary Schools: Teacher's Perspective and Experience. Corwin Press.
29. Willard, N. 2000. Legal and Ethical Issues Related to the Use of the Internet in K-12 Schools, 2000 BYU Educ. & L.J. 225 (2000). Available at: https://digitalcommons.law.byu.edu/elj/vol2000/iss2/5 (Accessed 16 April 2025).
30. Zong, J, Qui, J, Sun, M, Jin, X, Zwang, J, Guo, Y, Jin, X, Guo, Y, Xu, Y, Huang, J and Zheng, Y. 2022.To be Ethical and Responsible Digital Citizens or Not: A Linguistic Analysis of Cyberbullying on Social

Media. Sec. Educational Psychology. Vol.13:1-18. | https://doi.org/10.3389/fpsyg.2022.861823 (Accessed 15 March 2025).

31. UCT. 2025. Thandi's Story: The Terror of Cyber-Stalking (Based on the True Story). https://icts.uct.ac.za/services-security-security-resources-general-cyber-security/thandis-story-terror-cyber-stalking-based-true-story (Accessed 11 March 2025).
32. UNICEF. 2025. Cyberbullying: What is it and How to Stop it: What Teens Want to Know About Cyberbullying. https://www.unicef.org/end-violence/how-to-stop-cyberbullying#11 (Accessed 10 February 2025).
33. USA Attorney Office: Northern District of Dakota. 2021. Virginia Man Sentenced for Cyberstalking Tulsa Mayor. https://www.justice.gov/usao-ndok/pr/virginia- man-sentenced-cyberstalking-tulsa-mayor (Accessed 11 February 2025).