ACSI
Association of Christian Schools International
SOUTHERN AFRICA

ACSI Recommended Reading

Guidelines on e-Safety in Schools DBE



Guidelines on e-Safety in Schools:

Educating towards responsible. and ethical use of ICT in education



basic education

Department:
Basic Education
REPUBLIC OF SOUTH AFRICA

Read to Lead
A Reading Nation is a Leading Nation

2030 NDP

Guidelines on e-Safety in Schools: Educating towards responsible, accountable and ethical use of ICT in education

FOREWORD



Technology has become all pervasive both globally and locally and is providing citizens all over the world with a hitherto unknown access to information, communication and technology tools. ICT is the landscape in which the Information Age exists and with it brings the necessity for the acquisition of new skills and a cognitive understanding of how to manage the environment to ensure a productive outcome. There are endemic risks to using technology and e-safety education is pivotal in ensuring that learners, teachers and also parent/care-givers are fully equipped to anticipate potential harmful practices and to mitigate the same.

The Department of Basic Education recognises that it has a responsibility to ensure access to the ICT environment if our education system is to be relevant and in keeping with current practices globally. Access to the rich educational resources and professional communities of practice ensure participation and sharing, also that the system remains responsive and dynamic. Furthermore, we are ensuring that through the development of ICT skills and knowledge we are creating global citizens in both learners and teachers who can hold their own internationally. The integration of ICT in education has evolved with ever more sophisticated tools, and as participation and transition rates to higher levels of education increase, children and adults will increasingly need to develop digital literacy, not only for life skills but also to support their education throughout all levels; secondary, post-secondary and tertiary. The early integration of ICT into primary and secondary curricula through formal recommendations is therefore vital, and moreover acts as an important lever for ensuring the introduction and implementation of ICT into educational institutions and classrooms.

The concept of digital citizenship; i.e. responsible use of technology, is relatively new, but is an important concept especially for new users who might not realise the implications of cyberspace interactions, especially in terms of social media and online bullying.

The Revised Guidelines ensure that current practice in ICT in education is provided within a framework that promotes a safe and caring environment for learners and teachers. Furthermore, it ensures the delivery on our constitutional and educational imperatives such as protection of human rights, redress and equity, social cohesion, resource provision, flexibility of access, accountability, independent learning and learner support.

It is essential that a whole-school approach be followed with the implementation of these Guidelines by involving all relevant stakeholders at schools and that schools are supported by Provincial and District ICT officials.

MS A MOTSHEKGA

MINISTER, MP

DATE:

Table of Contents

	FOREWORD	2
1.	Introduction	6
2.	Purpose	7
3.	Background	7
4.	Scope	8
5.	How to best use these guidelines	9
6.	Acronyms	9
7.	Glossary and Definitions	10
8.	Acknowledgements	15
9.	Regulatory Framework	16
10.	Advantages of ICT access in schools	17
11.	Issues of concern regarding ICT access in schools	17
11.1.	Inappropriate or illegal online behaviours	20
11.2.	Physical danger and sexual abuse	20
11.3.	Exposure to unsuitable materials	21
11.4.	Plagiarism and copyright infringement	22
11.5.	Obsessive use of the Internet	23
12.	Responsibilities	23
12.1.	The Responsibility of the School	24
12.2.	The Responsibility of the Teacher	25
12.3.	The Responsibility of the Learner	26
12.4.	The Responsibility of the Parent/Guardian	26
13.	Strategies for managing ICT access in schools	27
13.1.	Acceptable Use Policies (AUP's)	28
13.2.	School Software Security	29

13.2.1.	Antivirus Software	29
13.2.2.	Monitoring software	30
13.2.3.	Document Security	31
14.	Conclusion	32
15.	References	32
16.	Some Internet sites	33
17.	ANNEXURES	35
17.1.	ANNEXURE A Examples of Acceptable Use Policies	35
17.2.	ANNEXURE B Information sheets	35
17.3.	ANNEXURE C What is Copyright?	35

1. Introduction

An ever-increasing use of technology in society, both globally and locally, has allowed easier, faster and cheaper access to Information and Communication Technologies (ICTs) like never before. This has resulted in digital 'citizens' of all ages having to acquire a new skills-set not taught using traditional methods and media. The pervasiveness of technology is often negatively publicised and the education system is responding positively by equipping all role players (teachers, learners and parents/guardians) with guidelines around the ability to recognise potential dangers and be discerning enough to avoid them.

The advantages of using ICTs for education far outweigh the disadvantages however; the latter need to be managed thoughtfully and responsibly in order to ensure the protection of our children. It is essential that schools are aware of how to manage the technology environment so that their learners have positive and safe experiences when using it and the learners, in turn, need to understand the implications of irresponsible use and need to be accountable for their behaviour. This can be done through proper Information Security (IS) education and awareness within schools.

It is essential that IS education is not confined to awareness of the risks and dangers of ICTs, but also includes an understanding of the benefits. The Safe School Committee[1] (comprising of all relevant stakeholders including school management), prescribed by South African Schools Act [2] should consider that while there are real dangers, too many limitations and controls can significantly decrease the positive aspects of access to technology. It is also essential that parents and guardians also need to share the responsibility as access to technology is not confined to the school walls, or solely to the time spent in the school environment.

The focus of the White Paper on e-Education[3] published in 2004 recognises the role that ICT can play in education, and by extension in lifelong learning and the development process. The larger society benefits from electronic education

1 Department of Basic Education Draft School Safety Policy 2010
2 South African Schools Act No 84 of 1996
3 White Paper e-Education 1994

(e-Education) include learning-for-life, the communication and exchange that are essential to democratic living, and globally competitive human resources.

As South Africa improves access through affordable hardware, software and connectivity, so must guidelines be in place for proper implementation and management thereof.

2. Purpose

The e-Safety Guidelines seek to identify the different ICTs currently used by school communities in particular, teachers and learners and to recommend strategies around managing ICTs in order for the appropriate and optimum use in, and for, education. This can be done by identifying all role players involved and their role and responsibility toward electronic safety (e-safety).

3. Background

Media and technology are evolving at a rapid pace, bringing opportunities, challenges and risks that are new to this generation. We are living in a world of rapid change, economically, politically, socially and technologically. The advent of improved connectivity and thus access to ICTs (for example the Internet and cell-phones) highlights the necessity for strategies to be in place in order that school communities have a positive, safe and fruitful experience of utilising technology.

Cell-phones in particular, are endemic in this country having a far-reaching footprint, even in the most rural of areas, so education needs to be a step ahead in ensuring that learners are equipped to manage both the risks and the benefits.

The Internet is a largely un-policed environment; anybody can upload information either authentic or not, unlike a traditional library whereby books go through an editorial process thus ensuring quality of information. We therefore recognise the need to teach our learners information literacy skills and these include digital literacy. Finding, selecting and using information effectively and appropriately are essential in the information age. Teaching our learners to use the most

appropriate communication tools for productive and wholesome interactions, as well as the development of their critical thinking skills, is a responsibility of teachers and parents/ guardians.

Equally, social network platforms provide unprecedented opportunity for building contacts and staying in touch with current events, developing an online identity for socialising, but the environment needs to be managed so that it does not predominate in the life of a learner.

It is essential that the value of the various platforms, devices and mediums is embraced in schools but it is equally important that education around the use thereof is intensive and thorough. Information literacy, and thus digital literacy, is about knowing what is available technologically speaking and selecting the most appropriate tools to find and communicate information in the most efficient, effective, responsible, safe and appropriate way possible. These are the skills required of the 21st century learner and global digital citizen.

Finally ethical use of information and communication platforms is a key aspect of education. The principles inherent in the Constitution and cited in the Bill of Responsibilities for the Youth of South Africa[4] are applicable in the online environment as anywhere else. Building the culture of responsibility, accountability and humanity in our schools also has application in the information age. Learners are, on the whole, proficient users of technology but are not necessarily world-wise, it is for this reason guidelines are necessary.

4. Scope

The guidelines for e-safety in schools apply to all learners, teachers and school management, including School Governing Bodies (SGBs), within the context of schools in South Africa. These guidelines should also assist parents/guardians to ensure that their children are e-safe. Provincial Department of Education officials and District officials should also be familiar with the document, and support the implementation of it in schools.

4 A Bill of Responsibilities for the Youth of South Africa 2008

5. How to best use these guidelines

The Department of Basic Education (DBE) acknowledges that while it is important to formulate guidelines on safety in schools, this document cannot be a comprehensive document to address all matters of safety in schools.

The DBE like to acknowledge other contributions by Educationalists, other Government departments and private sector to fully research, comprehend and address the challenges related to e-safety in schools.

The DBE thus would like to see this document to form part of, and enhance other projects with the same objectives. In practice this implies that the DBE would like to refer the readers of this document to also take note of the Digital Wellness Toolkit that was developed by the ACEIE, University of Pretoria and Intel. This toolkit complements the guidelines as set out in the e-Safety guide for schools, by providing practical ideas of implementation.

6. Acronyms

Acronym	Definition
AUP	Acceptable Use Policy
CSRT	Cyber Security Policy
DALRO	Dramatic, Artistic and Literary Rights Organisation
DBE	Department of Basic Education
DVD	Digital Versatile Disk
FAQ	Frequently Asked Questions
FET	Further Education and Training
FPB	Film and Publications Board
GET	General Education and Training
ICT	Information and Communication Technology
IS	Information Security
IT	Information Technology

Acronym	Definition
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
SAMRO	Southern African Music Rights Organisation
SAPS	South African Police Services
SGB	School Governing Body
SMS	Short Message Service
URL	Uniform Resource Locator

7. Glossary and Definitions

- Asynchronistic or Asynchronous: occurs at different times e.g. e-mail conversations.
- Blogs: Weblogs (blogs) are online journals created by individuals or groups and stored on the Internet. They are usually text-based, but also include other media such as images, video and sound content. Blogs are an ideal space to write about personal ideas and opinions.
- Browsers: tools to access the World Wide Web
- Cloud computing: term used to describe delivering hosted services such as infrastructure, platform and software services to other devices on demand. It lessens the workload on the local machine (the computer that the user is using).
- Communities of Practice (CoPs): a group of people who have a common interest or profession and who communicate and share information.
- Creative Commons licences: a licensing system for creative content such as video, audio or text, which specifies to what extent other people may share content, modify it, or give it away for free, and to what extent they are obliged to acknowledge or credit the original authors.
- Cyberbullying: Harassing, humiliating or threatening someone in cyberspace, by sending them nasty e-mails, posting malicious information, fake profiles or embarrassing photographs or comments on

social networking sites.

- Cybercrime: computer crime or cybercrime is a form of crime where the Internet or computers are used as a medium to commit crime.
- Cyberspace: The same as “Internet”: the global network of interconnected computers and communication systems.
- Cybersecurity: computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
- Cyberstalking: individuals who keep track of other users’ activities and information for no legitimate reason.
- Dark Web: is World Wide Web content that exists on dark nets, networks which overlay the public Internet and require specific software, configurations or authorization to access and are often used for illegal or criminal activity. The Dark Web forms part of the Deep Web, the part of the Web not indexed by search engines. Wikipedia [Accessed August 2015]
- Digital image: an image created by digital technology such as a digital camera, or imaging editing software.
- Digital Literacy: the ability to find, discern, select and use online information appropriately.
- Digital footprint: the collection of data, which includes images, videos and text, posted by an individual online.
- e-Education: consists of e-Learning, e-Teaching, e-Awareness and all the administrative responsibilities connected to these actions.
- e-Learning: a broad term that generally refers to any kind of learning that is done with a computer and Internet connection or other media like a CD-ROM. It is widely used by individuals, educational institutions and

businesses. e-Learning includes m-Learning.

- e-Mail: electronic mail, most commonly abbreviated e-mail and e-mail, is a method of exchanging digital messages.
- Filtering: a process to deny access to certain websites or resources as defined in the filter.
- Firewall: part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
- Flaming: hostile and insulting interaction between Internet users.
- Internet: a worldwide network that connects smaller networks together.
- Information literacy: the ability to recognise the need for information; to find, organise and evaluate such information for effective decision making or problem-solving, to generate new knowledge and to apply these skills for effective life-long learning.
- Information skills: the skills which underpin a learner's ability to define the purpose of an information task, locate resources of data, select, interpret and use information to complete a task.
- IT (Information Technology): defined as the "study, designs, expansion, execution, preservation or supervision of computer based information systems, specifically on computer hardware and software functions."
- ICTs (Information and Communication Technologies): defined as forms of technologies that are used to create, store, share or transmit, exchange information; radio, television, video, DVD, telephone (both fixed line and mobile phones), satellite systems, computer and network hardware and software; as well as the equipment and services associated with these technologies, such as videoconferencing and electronic mail (UNESCO 2002).
- Inter-operability: the degree to which different types of software and hardware can interact effectively with each other.
- Malware: a malicious or intentionally or unintentionally damaging software programme.

- Media: the means whereby the messages and images that we consume and create are transmitted. These include television, movies, video games, books, magazines, the Internet, cell-phones, advertising billboards, and more.
- m-Learning: a broad term that generally refers to any kind of learning that is done with a cell-phone, supplied directly on the cell-phone, as an application, game or similar content – or accessed via the Internet.
- Multimedia: media that combines two or more media of communication (text, graphics and sound etc.)
- Netiquette: Netiquette is a set of social conventions that facilitate interaction over networks, such as mailing lists to blogs and forums. These conventions include actions not to be used online, such as flaming people (see above), cross-posting (posting adverts on multiple platforms), or trolling (provoking people).
- Phishing scams: is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- Plagiarism: “the wrongful appropriation, close imitation, or purloining and publication, of another author’s language, thoughts, ideas, or expressions, and the representation of them as one’s own original work”. Wikipedia [Accessed August 2010].
- Social Media: Interactive media or websites which permit interaction between users, to promote user-generated content or communications. Examples include blogs, Facebook, Twitter, and similar. Social Networking: online platforms that provide means of personal communications between participants such as FaceBook, LinkedIn, Twitter, WhatsApp and many others.
- Spam: is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.

- Spoofing: Spoofing, or decoying, is the practice of inundating online networks with bogus or incomplete files of the same name in an effort to frustrate traders and reduce unlawful downloading. It can also refer to any falsification, e.g. of a domain name, so as to redirect traffic to another location.
- Synchronistic or Synchronous: things which occur at the same time e.g. online chat.
- Trolling: To provoke people online by deliberately making inappropriate, false, or unprofessional statements, so as to elicit a negative reaction.
- URL (Uniform Resource Locator): address that identifies a specific website e.g. http://www.education.gov.za.
- Viral branding: refers to marketing techniques that use pre-existing social networks to produce increases in brand awareness or to achieve other marketing objectives (such as product sales) through self-replicating (viral) processes.
- White-list: An approved list; often used with regard to Internet content filtering, a whitelist only includes addresses (such as URLs or e-mail) that have been specifically vetted in advance. Whitelists specify which protocols, sites or persons are allowed to communicate, unlike blacklists which specify which protocols, sites or persons may NOT communicate.

8. Acknowledgements

External advisors

Africa Centre for Excellence in Information Ethics (ACEIE)	Meraka Institute
Child Welfare SA	Microsoft
Cyanre	MTN SA (Pty) Ltd
Department of Home Affairs	MXit
Department of Justice and Constitutional Development	Oracle
Department of Social Development	SA Law Reform Commission
Department of Telecommunications and Postal Services	SchoolNet
Film and Publications Board (FPB)	South African Police Service (SAPS)
Intel	Vodacom

Department of Basic Education

Directorate: Curriculum Innovation
Directorate: FET Schools
Directorate: Gender Equity
Directorate: School Safety and Enrichment Programmes

Critical Readers	
Ms J Batchelor	Head IT Integration Cornwall Hill College
Ms M du Toit	Independent
Dr E Kritzinger	Senior Lecturer: School of Computing UNISA
D Nicholson	Copyright Services librarian: University of the Witwatersrand, Johannesburg
Dr P Miller	Pinelands High School

Dr H Vermeulen	University of Cape Town
Ms M Verster	Educational Technologist
Mr S Vosloo	Shuttleworth Foundation

9. Regulatory Framework

Legislation

Act No. 11 of 1967	Performers' Protection Act
Act No. 42 of 1993	Animal Matters Amendment Act
Act No. 108 of 1996	Constitution of the Republic of South Africa
Act No. 65 of 1996	Films and Publications Act
Act No. 84 of 1996	South African Schools Act
Act No.13 of 2000	Independent Communications Authority of South Africa Act
Act No. 70 of 2002	Regulation of Interception of Communications and Provision of Communication-Related Information Act
Act No. 36 of 2005	Electronic Communications and Transactions Act
Act No. 38 of 2005	Children's Act
Act No. 31 of 2007	Education Laws Amendment Act
Act No. 32 of 2007	Criminal Law (Sexual Offences and Related Matters) Amendment Act
2008	A Bill of Responsibilities for the Youth of South Africa
B9 – 2009	Protection of Personal Information Bill

Policies

2010 Cyber Security Draft Policy: Department of Communications

2015 School Safety Policy: Department of Basic Education

10. Advantages of ICT access in schools

In the South African context, the concept of e-Education revolves around the use of ICT to accelerate the achievement of national education goals. e-Education is further about connecting learners to other learners, teachers and related professional support services. e-Education connects learners and teachers to more information, ideas and one another via effective combinations of pedagogy and technology. The challenge is to transcend mere exchange of information and to transform it into a range of learning activities that meet educational objectives. e-Education is more than developing computer literacy and the skills necessary to operate various ICTs; it is the ability to apply ICT skills to access, manage, integrate, evaluate, and create content in order to enhance teaching and learning and to function in a knowledge society. ICT-capable learners are able to access information in the digital era, manage information effectively, interpret and integrate the results of research, evaluate the quality of these results, and create new content by adapting, applying, designing, inventing, or authoring information.

Success in the infusion of ICT into teaching and learning will ensure that every learner will be equipped for full participation in the knowledge society before they leave school. These learners will use ICTs to enhance interaction between citizens, governmental organisations and public and elected officials. These learners will invent new ways of using ICTs to realise the Department of Basic Education's vision of developing a lifelong learner who is a critical and an active digital citizen and who embodies the fundamental values of the constitution.

11. Issues of concern regarding ICT access in schools

1.1. Online harassment and cyberbullying

Some aspects of digital communication can give rise to unfortunate behaviour. These include;

- The ability to communicate anonymously and so to escape responsibility

for one's actions.

- The ability to communicate remotely thus not having to deal with a "face to face" confrontation where the normal rules of politeness might inhibit unpleasant behaviour.
- The public nature of social media and social networks, which makes it easy to publicly humiliate an individual with little or no consequence.
- An invasion of privacy if messages sent to/from an individual are released into the public domain

Cyberbullying can include the repeated sending of unwanted communication; as well as the posting of offensive statements about other learners or about teachers using any of the digital mediums that can make learners, and teachers, feel embarrassed, upset, depressed, or afraid. Groups and cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member, can quickly escalate into something much more serious.

It should be made clear to all that bullying using digital means is still regarded as bullying and carries serious consequences according to the Acceptable Use Policy of the school. It must be noted that bullying of any kind is a social problem and is thus a whole school responsibility. Normal courtesy and good manners apply as much in the cyber world as the real world.

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal information	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting Personal information	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal: Downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

11.1. Inappropriate or illegal online behaviours

Young people may get involved in other inappropriate, anti-social or illegal behaviour while using new technologies. The teaching of appropriate behaviours and critical thinking skills to enable learners to remain both safe and legal when using the Internet and related technologies is essential. Young learners who have been engaging in risky or illegal behaviours online may benefit from professional support or counselling to address the balance of their online and offline life. Some children may become involved in much more serious activities. Possible risks include;

- Involvement in identity theft;
- Participation in hate or cult websites;
- Buying and selling of stolen goods and drugs;
- Participating in inappropriate sex-related online activities or “grooming”;
- Divulging personal information online; and
- Publishing compromising information which may harm an individual’s reputation

Learners should be aware of the consequences of leaving “online tracks” often called a Digital Footprint i.e. information about themselves that may damage their reputations and employment opportunities later on.

It is also essential for learners to take charge of protecting their own privacy, and avoid posting any information which can be used by identity thieves. Identity theft is a very real risk that has a significant personal and financial cost. Learners should be made aware of safety and privacy measures that exist on social networking sites; these can include a “Report Abuse” button, safety tips, age restrictions, built in privacy controls etc.

11.2. Physical danger and sexual abuse

A criminal minority make use of the Internet and related services such as “chat-rooms” to make contact with young people. The intention of these people is to

establish and develop relationships with young people with the sole purpose of persuading them into sexual activity and exploitation. “Cyber stalking” is where individuals keep track of the activities of certain people through their participation on social networking sites. This can result in physical stalking if their whereabouts are revealed online. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online friendship. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging as a prelude to a meeting in person. This can even culminate in persuading a young person to forward explicit photographic images of him/herself or another young person, or even just to participate in communication of a sexual nature. These techniques are examples of criminal conduct and adult persons who commit such acts can be convicted of the “sexual grooming” of children.

A young person needs to understand that it is unwise to supply personal information, pictures of an explicit nature or arrange to meet people they have met online, thereby posing a risk to their safety or that of their family or friends. Furthermore, the online world offers a degree of anonymity and the online persona of a person, under these circumstances, can be far removed from reality.

11.3. Exposure to unsuitable materials

Exposure to inappropriate materials poses a risk when using the Internet. This may include, but is not limited to, material that is pornographic, hateful or violent in nature, activities that are dangerous or illegal, or material that is just age-inappropriate or biased. One of the key benefits of the Internet is that it is open to all, but unfortunately this also means that those with extreme views are able to share their ideas without restriction or consideration of other views. In the case of pornography the Internet plays host to a large amount of material. Curiosity about sexuality issues is a normal part of sexual development, but young people may be shocked by some of the overtly explicit material online. The ease of access to adult sites such online gambling, making and sale of

weapons, and sites providing recipes for drug or bomb making are also of great concern. This space is often referred to as the “Dark Web”.

Through mobile devices such as cell-phones and tablets, young people may themselves become perpetrators in the creation of inappropriate content by the making and distribution of indecent images, videos and derogatory lists. They also might not actually create the content but may view and thus be exposed to unsuitable material or be the victim of such abuse of technology.

11.4. Plagiarism and copyright infringement

Copyright law applies on the Internet, but is ignored by many young people who download and swap music files, “cut and paste” homework assignments from other’s work, purchase whole assignments from online “cheat sites” and are doing so without realising the implications and consequences. The school needs to ensure that assignments are given in such a way as to not invite a “cut and paste” response but have activities within that require primary research, problem-solving and other higher-order thinking skills as opposed to merely superficially ‘grazing’ for information. Learners must be taught that credit must always be given to the source of information and pirating music, images, videos or software is not only unethical but is dishonest and illegal. Available referencing and citation programmes can help instil correct research methodology, and teachers should critically evaluate what is expected from the learner.

Social networking platforms have created an environment whereby information is shared without necessarily giving credit to the source. The democratisation of information i.e. where everybody has an equal voice, is one of the most valued aspects of recent technologies. It has however, blurred the edges of respect for intellectual capital, and anybody who ventures into the environment needs to understand that their opinions might not necessarily be credited to them.

11.5. Obsessive use of the Internet [5]

Habitual use or addictive behaviour in the online world creates the potential for learners to become obsessed with the Internet or cell-phone chat services and related technologies. Factors such as spending a significant amount of time online, deterioration of the quality of schoolwork, diminished sleep time, or negative impacts upon family relationships, may all be indicative that the online world is taking too high a priority in a young person's life and can intrude excessively if not managed properly.

Another aspect of misuse of the technology is the circulating of band-width intensive e-mail (large file attachments) which are unrelated to the school working environment, chain letters etc. Beyond compromising the speed of connectivity, the time taken on managing inappropriate and personal activities during school working hours can be costly to the performance of both the learner and teacher.

A further concern which can raise cost and health issues is data hoarding and obsessive watching of YouTube and other online videos. It is quite commonplace nowadays to find that children watch, download and collect video and music files. This has cost implications for parents who pay for the bandwidth. Parents need to monitor their children's online video habits and not allow electronic devices to become even more engrossing versions of televisions. Children need to be encouraged to play outside, read physical books, and engage directly with physical persons, too.

12. Responsibilities

Although these guidelines have been written specifically with schools in mind it is also essential that parents, Provincial and District officials take cognisance of the content and apply it in their own situation where relevant. Ethical and accountable use of technology applies at district level as well as in the schools. They should also support the school in implementation of the guidelines.

5 Safer Children in a Digital World: the report of the Byron Review - Children and New Technology 2008

12.1. The Responsibility of the School

Technology, as per its broadest meaning, has an imperative role in today's classrooms. The use of that technology, however, must be carefully and strategically implemented in order to be of highest value to both teachers and learners. Technology use has a place in formal and informal learning; it does not only happen in the classroom but outside of the school environments. Traditional controls no longer exist and schools need to embrace the potential of technology for learning through using appropriate measures.

Recognising that the use of technology will increase exponentially in all our lives, the responsibility of the school is to not only incorporate technology as a valuable learning tool, but to also equip the learners to be discerning, responsible and ethical participants in the information age.

Through the Safe School Committee schools must develop their own Acceptable Use Policy (AUP), as it must be recognised that children will bring an increasingly sophisticated range of handheld devices into school giving them separate access to content that is not necessarily appropriate. The AUP should be linked to, and the penalties defined by, the existing Code of Conduct[6] that must be adopted by every public school.

The AUP should clearly define the penalties imposed for violation of the agreement and this should be read and signed by every learner and responsible parent or guardian. The school must keep the copies signed by the learner and the parent/guardian and all signatories should have access to a copy via the school Intranet or otherwise. A simplified version of the AUP should be posted in the staffroom and also on the screen of all the computers. In order to create a sense of personal responsibility it is important that wording is values-based as opposed to rules-based.

As misuse of technology is not necessarily confined to learners. Schools can elect to have a similar policy for teachers. The AUP policy of a school will have to be revisited once the Protection of Personal Information Bill, 2009, is enacted. The Bill aims to regulate the processing of personal information by public and

6 South African Schools Act (Act No 84 of 1996 amended 2007)

private institutions and will, among others, regulate unsolicited electronic communications such as “spam”. An Information Regulator will be appointed to oversee the implementation of the legislation. AUP policies may, therefore, in future, have to be adapted with the assistance of the DBE and Information Protection Regulator to ensure that they are brought in line with the legislation concerned, where necessary.

12.2. The Responsibility of the Teacher

Teachers have a specific responsibility in terms of the use of ICT in schools. Partnership for 21st Century Skills[7] specifically refers to information literacy as well as ICT literacy. Learners are increasingly using their cell-phones to communicate, share and find information and teachers need to understand the concept of the 21st century learner, especially to ensure that their teaching strategy is in line with the devices their learners use. Teaching and learning can be greatly enhanced with increased access to communication and information and this potential needs to be maximised by teachers. Integrating technology appropriately into teaching practice is important; a ‘just-in-time’ approach within a contextualised learning environment versus “just-in-case” i.e. learning computer skills in case they may be needed in the future. An additional responsibility of the teacher is thus to make sure that they themselves are digitally literate and can educate around the technology with confidence.

Teachers can direct learners to age-appropriate content and websites; they can also create White Lists of carefully selected websites appropriate to the topic and the age group. Telling learners to “Google” a topic i.e. use a single search engine to find information is the equivalent of exposing them to a massive library with no information retrieval skills, furthermore the most benign topic can elicit inappropriate material. Teachers should be made aware of Google’s “safe search” option which filters most adult content out.

It is further suggested that teachers may need to provide guidance, counselling and advice to learners who may be dealing with harassment, stalking, cyberbullying etc.

7 Partnership for 21st Century Skills http://www.p21.org/

A further aspect of the responsibility of the teacher is to not abuse access to technology for personal matters, doing time-consuming non-work related activities, circulating bandwidth-intensive files and images which do not benefit the learners or the school, using school printers for personal use etc. Leading by example in the ethical use of technology goes a long way in educating learners.

12.3. The Responsibility of the Learner

Learners today are navigating social networking websites, downloading music, uploading photos and videos, e-mailing, blogging, building personal websites, and playing online games with people from around the world. Online and user-generated media, whether it is television, cell-phone, online games or videos is especially challenging because there are few barriers to what can be posted and made available, and that can make offensive content readily available.

Learners are however, at different levels of sophistication and this can negate a positive global experience. The nature of technology, especially interactions predominantly in a second language for the majority of our learners, can give rise to misinterpretation and misunderstandings.

Learning to take responsibility for one's behaviour is an important element in the education path and this includes the use of technology. The ease of access can invite an inappropriate, spontaneous reaction and it is important that learners understand the need to select the most suitable communication tool to resolve issues and not create them. An aspect of taking responsibility in the environment is to report any inappropriate behaviour especially if offensive acts are negatively affecting a fellow learner.

12.4. The Responsibility of the Parent/Guardian

Parent and guardians have a responsibility to monitor the use of technology both in the home and outside of it. This is difficult to do, especially with cell-phones, but if children and young adults are educated around the use of technology and the education is values-based rather than rules-based, then this can go a long way to ensuring the healthy and balanced use of the devices.

It is possible to set up age appropriate content filters on Internet browsers and it is also possible to check the cache (browsing history) on a computer if it is felt necessary to do so. The technology enables parents/guardians to password protect either a computer or online facilities like “chat rooms” even through cell-phone access. This prohibits children of a sensitive age from accessing these areas.

There is filtering/monitoring software that can be downloaded but children and young adults need to be informed that their activity is being checked upon. It is important that the school is supported by the parent/guardian in respect of any sanctions imposed if the school AUP has been breached.

Parents/guardians are encouraged to disallow children from using or accessing the Internet in isolation or behind closed doors. A suitable family area should be set up for such usage and this includes access to television. Furthermore parents/guardians should discourage their children from publicly divulging personal information such as contact details and whereabouts.

13. Strategies for managing ICT access in schools

It is very important that a school sets up a team within the Safe School Committee to manage e-Safety and this team should consist of at least;

- School Management
- Network administrator
- IT teacher
- Teacher-Librarian/Counsellor/Life Skills teacher
- School Governing Body representative
- A member of the local police service
- Learner representative
- Other appropriate specialists

The function of the team is to develop, implement and enforce an Acceptable

Use Policy/ies (AUP) for the school with attendant penalties for breach of such a policy.

13.1. Acceptable Use Policies (AUP's)

It is strongly advised that each school, as part of the function of the Safe School Committee, develops an Acceptable Use Policy and all learners should be required to sign it, indicating that they accept the policy and related sanctions. Alternatively, two separate policies can be developed; learner-specific and teacher-specific. It is further advised that the Acceptable Use Policy/ies should include a clear statement of the actions which the school will take if the policy is breached. This will considerably strengthen the school's position should this situation arise.

The policy/ies should be endorsed by a credible legal service to ensure that it is implementable in terms of the legislation and also that Child Protection procedures are followed. South African Police Services (SAPS) has guidelines in this regard.

All role-players must be made aware of the content and consequences of the policy. Parents/guardians should take all reasonable steps to ensure that their children comply with the requirements.

There are basically three levels of issues surrounding the use of technology. First, there are the problems associated with nuisance in classes and disruption of learning and teaching. Second, there is the type of incident, which has potentially criminal implications. Third, there are incidents with specifically child protection dimensions. An Acceptable Use Policy must therefore address all three levels.

The suggestion is offered that the policy might explicitly cover the following:

- The school's responsibility and rights towards ICT use;
- The learner's responsibilities and rights towards ICT use;
- The parent/guardians responsibility and rights towards ICT use; and

- The consequences if the policy is not adhered to.

It is stressed that in cases, which are disciplinary in level, school disciplinary procedures (including exclusions when required) should be used proportionally and appropriately. In other cases, it is best for schools to work constructively with parents/guardians. In connection with these issues, the normal rules and protocols apply with regard to the rights of schools to take action over behaviour, which is school-related but which actually occurs out of school. For example, if a child posts an offensive message about his or her school after school hours on a site which is not related to the school itself, that will still constitute an offense in terms of the AUP, even though it was not done during school hours on school property.

13.2. School Software Security

There are several ways that a school can manage online security and it is important that a strategy is in place. The two main elements are to ensure that school computers are protected from viruses and malware and also that online behaviour on the part of learners and teachers is managed.

13.2.1. Antivirus Software

Antivirus software should be installed on the school server/individual computers where applicable[8] . Not only should the software definitions be updated on a regular basis, but the computers should be regularly scanned, if applicable. Furthermore peripherals such as memory sticks/flash drives, external hard drives etc should also be scanned as this is a common way for viruses to be introduced into a system.

Proprietary antivirus software normally entails the payment on an annual licence fee and this range from a single-user licence to multiple-user licence.

8 Not all systems require this software, e.g. it does not particularly apply to many mobile computing platforms.

There are free antivirus software programmes available on the Internet. Furthermore there are online detection programmes which scan computers whilst linked on the Internet. Be aware that some of these services are in fact fake services designed to defraud you (e.g. when you get a banner that comes up saying 'Your computer has a virus', and you know that you've just scanned it and not found one). You should use online virus scanners only if they are reputable and recommended by an ICT professional.

It is vital that antivirus software is current and regularly updated, checked and computers are scanned. There is no use in having antivirus software if it is not properly managed.

13.2.2. Monitoring software

This can be installed on computers so that online activity can be monitored. There are many commercial programmes available as well as Open Source classroom management programmes.

A programme should be selected on the basis of controlling online behaviour through documenting and recording for the purpose of pastoral intervention versus punishment and/or banning. Users (learners and teachers) must be informed at the outset that their online activity is being monitored. The purpose is to provide a safe online environment which educates users how to manage their access. It is important to remember that the Constitution of the Republic of South Africa (1996) guarantees all citizens the right to privacy. Therefore, controlling online behaviour must not overstep the bounds of reasonable respect for privacy.

In addition to informing users (learners and teachers) of the fact that monitoring is taking place, they should also be informed, within the AUP, of the following:

- Exactly what data is captured by the monitoring software?
- How long is this data kept
- Who has access to this data

- How the data will be kept safe so that unauthorised users cannot access it
- What mechanisms there are to ensure the data is accurate
- How this data can be used.

The issues discussed above must be set out and explained in the AUP.

Teachers and principals should also bear in mind that whatever technologies they put in place on the school LAN or the school computers, are in fact completely moot and ineffectual if the learners are using their own personal devices. Learners cannot, for example, legally consent to having monitoring software installed on their own devices (as they are legal minors). And further to this, there is realistically nothing that can be done to prevent learners from using their own devices, certainly during break times. It is therefore proposed that the AUP promotes the good reasons for safe online conduct, rather than emphasising rules and punishments for breach of the rules.

13.2.3. Document Security

In keeping with the points in 12.2.2, included in the AUP should be a reference to document security and the confidentiality of school documentation. It is known that businesses have been compromised through the deletion or inappropriate copying or forwarding of information and this has to be a consideration for schools. A system for password access for different user groups needs to be created and certain documents need to be secured, either password protected or using software such as Adobe Acrobat. Information security requires that information on learners stored on the school network is secure, especially demographic and identity information.

Computer hacking by mischievous learners is another element of school ICT security and it is for this reason that the identity of all users is kept secure. It must be impressed on learners that their password is confidential and that they must log off before leaving a school computer.

It is also advisable that an on-site and off-site backup of all the school data is kept and is regularly updated. Hardware failure happens as does theft and fire. The backup also needs to be tested on a regular basis.

14. Conclusion

Through the development and implementation of these guidelines it is hoped that schools are equipped to manage ICT in a positive and productive way. ICTs are part of the lives of the 21st century learner and will increasingly impinge on society. There is no choice but to embrace the attributes of technology and use them to enhance the education, communication and knowledge acquiring process. The Department of Basic Education wants to develop global digital citizens who are confident users who collaborate and participate but who know the boundaries and respect decent behaviour.

15. References

Byron, T. 2008 *Safer Children in a Digital World: the report of the Byron Review - Children and New Technology* [Online]. Available: http://www.dfes.gov.uk/byronreview/ [22 August 2010]

Digital Wellness Toolkit. 2015. ACEIE [Online]. Available: http://www.up.ac.za/en/african-centre-of-excellence-for-information-ethics/article/2109737/digital-wellness-toolkit

Palfrey, J. et al 2008 *Enhancing Child Safety and Online Technologies: final report of the Internet Safety Technical Task force* (Berkman Centre for Internet & Society at Harvard University) [Online]. Available: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf[26 November 2010]

Prensky, M. 2001. *Digital Natives, Digital Immigrants*. From: *On the Horizon* (MCB University Press, Vol. 9 No. 50).

Trilling, B and **Fadel C**. 2009, *Partnership for 21st Century Skills: Learning for Life in Our Times.* Jossey-Bass. New York. (http://www.p21.org/)

White Paper on e-Education. 2004. National Gazette No. 26734, 26 August 2004.

16. Some Internet sites

Africa Centre for Excellence in Information ethics	http://www.up.ac.za/en/african-centre-of-excellence-for-information-ethics/article/2087741/open-access-material
Ask About Games	http://askaboutgames.com/
Becta e-Safety	http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/BEC1-15535.pdf
Bloxx Web Filtering and Content	http://www.bloxx.com
Byron Review	http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/Byron_Review_Action_Plan.pdf
Child Exploitation and Online Protection Centre	http://www.ceop.police.uk/
Child Exploitation and Online Protection Centre	http: www.thinkuknow.org
Childnet International	http://www.childnet-int.org/
Cyber safety and Security	http://www.intel.com/content/dam/www/public/us/en/apps/cyber-security-and-safety-toolkit/index.html
Cyber safety	http://www.safetnet.com
e-Safety	http://www.wisekids.org.uk/BECTA%20Publications/esafety.pdf

Forensic Software	http://www.forensicsoftware.co.uk
Impero Classroom Management	http://www.imperosoftware.com/
Internet Watch	http://www.iwf.org.uk
Internet safety India reference	http://scholastic.co.in/en/articles/guide-internet-safety-kids-8-10
Italc: Open Source Classroom management system	http://italc.sourceforge.net/home.php
Learning Curve Education Online Safety for Kids	http://www.learningcurve.info/ http://www.mcafee.com/us/about/corporate-citizenship/online-safety-for-kids.aspx
Online behaviour	http://www.safekids.com/kids-rules-for-online-safety/
MXit Safety Guidelines for Learners and Parents	http://www.mxit.com http://forum.mxit.com/viewtopic.php?t=1936
Plagiarism Advice	http://www.plagiarismadvice.org
South West Grid for Learning Trust	http://www.swgfl.org.uk/staying-safe
Wikipedia list of antivirus software	http://en.wikipedia.org/wiki/List_of_antivirus_software
Wits Plagiarism Portal	http://web.wits.ac.za/Library/ResearchResources/SubjectPortals/Plagiarism+Portal.htm
Wits Copyright Information	http://web.wits.ac.za/Library/Services/COPYRIGHT.htm
Wits Copyright Portal	http://web.wits.ac.za/Library/ResearchResources/SubjectPortals/Copyright+and+Related+Issues.htm

17. ANNEXURES

17.1. ANNEXURE A Examples of Acceptable Use Policies

17.2. ANNEXURE B Information sheets

17.3. ANNEXURE C What is Copyright?

ANNEXURE A: The Acceptable Use Policy (AUP) for ICT in a School

Developing an Acceptable Use Policy (AUP) for ICT in a school

The Acceptable Use Policy (AUP) for Internet use is one of the most important documents a school will produce. Creating a workable AUP requires thoughtful research and planning.

With the current push for computer technology in the classroom, many educators and parents fear dangers that the uncensored access to technology might hold for children: inappropriate or obscene words and images; violence; and people who pose an online threat.

One strategy that many schools use to defuse such dangers is an Acceptable Use Policy, or AUP, for the school.

WHAT IS AN AUP?

The Department of Basic Education suggests that an effective AUP contains the following six key elements:

- a preamble,
- a definition section,
- a policy statement,
- an acceptable uses section,
- an unacceptable uses section, and
- a violations/sanctions section.

The **preamble** explains why the policy is needed, its goals, and the process of developing the policy. This section should say that the school's overall code of conduct also applies to learner online activity.

The **definition section** defines key words used in the policy. Words and terms such as Internet, computer network, education purpose, and other possibly ambiguous terms need to be defined and explained to ensure learner and parent comprehension.

A **policy statement** must tell what computer services are covered by the AUP and the circumstances under which learners can use computer services. Schools may, for example, base learner access to computer services on the completion of a "computer responsibility" class that will enhance learner understanding of the AUP guidelines.

The **acceptable uses section** must define appropriate learner use of the computer network. It may, for example, limit learner use of the network to "educational purposes," which then must be defined.

In the **unacceptable uses section**, the AUP should give clear, specific examples of what constitutes unacceptable learner use. In determining what is unacceptable, the committee charged with drafting the AUP must consider:

- What kind of computer network sites, if any, should be off limits to learners;
- What kind of information sending, forwarding, or posting, if any, should be prohibited,
- What kind of learner behaviour will be destructive to the computer network services and should, therefore, be restricted.
- Ensure that learners understand and apply the feelings, rights, values and intellectual property of others in their use of technology in school and at home;
- Understand what action should be undertaken if they feel threatened, worried, uncomfortable, vulnerable or at risk whilst using technology.

Among the sites that might be off-limits to learners are chat rooms and examination paper vendors. In addition, AUPs often prohibit learners from sending, forwarding, or posting sexually explicit messages, profanity, and harassing or violent messages.

The **violations/sanctions section** should tell learners how to report violations of the policy or whom to question about its application. The AUP should provide that violations will be handled in accordance with the school's general learner code of conduct.

A typical AUP has a section where learners and parents sign the document, in acknowledgement that they are aware of learner's restrictions to network access and releasing the school of the responsibility for learners who choose to break those restrictions.

In a free and democratic society, access to information is a fundamental right of citizenship, and therefore independent learner use of telecommunications and electronic information resources will be permitted upon submission of permission forms and agreement forms by parents of minor learners (under 18 years of age) and by learners themselves. The message should thus be that learners have intellectual freedom based on their taking responsibility for accepting limits to that freedom.

SAFETY FIRST

AUPs should make learners aware of basic information and communication technology safety rules before they are allowed access independently. The rules should be considered to guide independent use by learners, such as:

- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I 'meet' online without first checking with my parent/guardian. If my parent/guardian agrees to the meeting, I will make sure it is in a public place and I will bring my parent/guardian.

- I will never send a person my picture or anything else without first checking with my parents.

It must be remembered that an AUP cannot be developed in a vacuum. A vital, workable Acceptable Use Policy must be based on a philosophy that balances freedom and responsibility. It should be a values-based document as well as that aimed at protecting the individual.

Schools must be prepared to:

- develop an 'acceptable use policy,' (AUP);
- provide examples of AUPs from schools and libraries;
- respond to inaccurate perceptions of inappropriate material;
- promote positive examples of use;
- understand software to block inappropriate sites and related safety/ censorship issues;
- contact organisations committed to electronic freedom of information; and
- ensure there are appropriate pre-screened resources available to learners.

Example 1: A PRIMARY SCHOOL INTERNET ACCEPTABLE USE POLICY

Name of School :

Section A: Expectations

Whilst the Information Technology (IT) department has many stringent checks and controls in place, the Internet is a vast and continuously growing arena and as such there are some sites and images that may escape the schools scrutiny and it is in this area that the children need to be responsible and educated in their responses.

Learners are responsible for their own behaviour on the Internet just as they are in a classroom, on the sports field or on the playground. Communications and interaction on the internet are often public in nature and general school rules for behaviour and communications will apply. This includes their interaction with other learners on social networking sites such as Facebook, MXit, Twitter etc. even if accessed from home, as they are still learners of name of school and are expected to uphold the ethos of the school.
The use of the Internet is a privilege, not a right, and may be revoked if abused.
Learners are personally responsible for their actions when accessing and using the school computer resources. Learners are advised never to access, keep or send anything that they would not want their parents / teachers or anyone else to see. It is expected that the learners will follow and comply with rules set out below.

Acceptable uses

As internet facilities are a limited resource and one for which the school pays, users are expected to use them primarily for:

1. Direct educational purposes
2. Accessing information for private interests or hobbies which are school-related
3. Constructive communication with other Internet users and email recipients

Section B: Unacceptable uses

Users are not to:

1. Take part in the sending or resending of chain letters.
2. Use bad, offensive or derogatory language, or participate in any activities which discredit another child, in any communications over the internet.
3. Attempt to access or send attachments of any pornographic or socially unacceptable content. This includes racist, violent, harmful and bullying content.
4. Use any other user's Email account or logon.
5. Attempt to spread viruses or download programmes or games or malware of any kind.

In addition, when using the school's network, internet and email facilities, learners must understand their responsibility and behave in the following manner:

1. All users are entitled to the privacy of their work and therefore it is an offence to use or attempt to use another user's account or password.
2. Should a site, email message or image manage to bypass the safety controls it is the learner's responsibility to close the item and report it immediately to a staff member, to enable the blocking of the material.
3. Storage capacity is at a premium and learners are encouraged to conserve space by deleting unnecessary emails or saved pictures and documents that take up space on the server.
4. Learners must in no way attempt to "hack into" or interfere with the normal running of any other computers or networks.
5. Learners have full responsibility for their user accounts and must not share their passwords with anyone other than their parents. If they do and their account is used for breaking any of the acceptable use policy and it is traced to their username they will be solely responsible as the owners of the account.
6. Learners must be aware that excessive usage and their internet activities are logged and can be traced.
7. Printing is costly and learners must be aware that they have the privilege of a printing account and should they exceed this by printing private matter they will have to purchase a "recharge" voucher.
8. The computer staff, general staff, management and the Principal reserve the right to investigate any child's email or Internet usage who, in their opinion may be transgressing any of the rules in this policy.

We have read this document, discussed and understood its contents and agree to abide by them:

Learner's name:_____ **Date:**_____

Learner's signature:_____ **Date:**_____

Parent's/ guardian's name: _____
Date:_____

Parent's/ guardian's signature: _____
Date:_____

Example 2: MODEL OF AN ACCEPTABLE USE POLICY FOR ICT IN A SCHOOL

The school's information technology resources, including email and Internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources:

Learners must:

- Respect and protect the privacy of others.
- Use only assigned accounts.
- Not view, use, or copy passwords, data, or networks to which they are not authorized.
- Not distribute private information about others or themselves.
- Respect and protect the integrity, availability, and security of all electronic resources.
- Observe all network security practices, as posted.
- Report security risks or violations to a teacher or network administrator.
- Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
- Conserve, protect, and share these resources with other learners and Internet users.
- Respect and protect the intellectual property of others.
- Not infringe copyright (not making illegal copies of music, games, or movies!).
- Not plagiarise.
- Respect and practice the principles of community.
- Communicate only in ways that are kind and respectful.
- Report threatening or discomforting materials to a teacher.

- Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
- Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
- Not use the resources to further other acts that are criminal or violate the school's code of conduct.
- Not send spam, chain letters, or other mass unsolicited mailings.
- Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

Learners may, if in accord with the policy above

- Design and post web pages and other material from school resources.
- Use direct communications such as IRC, online chat, or instant messaging with a teacher's permission.
- Install or download software, if also in conformity with laws and licenses, and under the supervision of a teacher.
- Use the resources for any educational purpose.

Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a learner's privileges to use the school's information technology resources.

Supervision and Monitoring

School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any learner or other person,

or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS:

_____	_____
Learner	Date
_____	_____
Parent/Guardian	Date

Parents please discuss these rules with your child to ensure he or she understands them.

These rules also provide a good framework for your child's use of computers at home, at libraries, or anywhere.

ANNEXURE B

The following are guidelines on different media platforms, tools and content including Copyright issues.

1. Television Programmes

Description: **Television (TV) is a** medium **for transmitting and receiving moving** images**, usually in colour and accompanied by** sound**.**

Uses: Television programmes can be used for education as well as entertainment. Documentaries, films and reality programmes can be used as a resource in the classroom as well as specially designed programmes aired to support the curriculum. At present there are existing education channels specifically to support education in South Africa.

Advantages: Television programmes can have a far reaching impact on learning. Well made, informative programmes can be an invaluable tool in ensuring an enriching and relevant learning environment. Locally developed programmes can be in the vernacular and contextualised for the local cultural and geographical environment.

Considerations:

- Access to television, especially subscription television is not always available to all learners and teachers.
- Advertisements can be intrusive and disruptive. They can also be inappropriate to the age of the learner.
- Licences for multiple viewers can be expensive.
- Programmes made in other countries do not always support local culture, language and traditions.
- Making television programmes is a time-intensive and expensive venture which means that the majority of programmes are imported.

- Not all programmes on television have been classified according to the appropriate age group etc.

Recommendations:

- Although access to television is mostly in the home, schools can invest in making television available.
- Television is a passive medium with no interaction and should be used appropriately and selectively.
- Programmes can be valuable especially those aired specifically for learners. Recordings can be made of these and broadcast at school however; copyright rules should be adhered to (see Annexure C).
- Programmes shown to learners should be properly classified by the Film and Publication Board.
- The school must comply with the Film and Publication Board classification as learners should not be exposed to inappropriate material.
- Schools must comply with the licence conditions of the SABC with the number of licences matching the number of television sets.
- The school's Acceptable Use Policy (AUP) should take cognisance of the regulations and have steps in place to ensure compliance.

2. Digital imagery e.g. film, video/DVD and photographs

Description: The term "digital image" both moving and still, refers to an image created with digital technology such as digital camera, digital video camera, scanners or image editing software.

Uses: Every aspect of education can be enhanced through the use of digital images – either still images such as photographs or moving images such as video or animations.

Advantages:

- Images in education convey a powerful message especially and are especially useful for second language learners.
- Images are further enhanced when combined with sound and movement.
- Many cell-phones can be used to create digital still images and video, which makes it easy to create and share.

Considerations:

- Sharing images may be a cause for concern when these images are of a violent or personal nature or in any other way inappropriate.
- The taking and sharing of such images could be an invasion of privacy of an individual as well as potentially harmful to the viewer, especially if not used within the context of learning.
- Schools can hire/buy/record/copy videos/DVDs and inadvertently be in breach of copyright, especially if the group is large and the material used is only for purposes of entertainment.
- Images can be downloaded from the Internet and this could also breach copyright.
- Video streaming and downloading of large images can be a large drain on network resources.

Recommendations:

- Programmes shown to learners should be properly classified through the Film and Publication Board and these should be complied with.
- There are limitations on the size of the group of viewers, the purpose of the viewing and also whether learners can be charged. The school needs to be familiar with these rules.
- If photographs or video clips are uploaded to the Internet, learners and teachers need to be aware of the need to protect the identity of the people portrayed, as well as the identity of the authors of the material. If any of

these are minors, it may be appropriate to take measures such as using only first names, or removing any information which could be used to track these individuals.

- Cognisance should be taken that some cultures do not permit images to be taken of people.
- Any image, whether still or video, may only be re-used with permission from the original copyright holder, or according to the terms of the Creative Commons licence if there is one.
- Teachers and learners should take cognisance of what images may be downloaded without breaching copyright.
- Credit should be given to the source of any digital material used for education purposes. Learners and teachers equally, should respect copyright.
- Schools should be aware that many brands are capitalising on the medium to promote their products and learners should be made aware of this.
- Permission from the parent/guardian can be included in the school's Acceptable Use Policy (AUP) if images of learners are to be used on the Internet.
- The school's Acceptable Use Policy (AUP) must specify where, when and what type of digital imagery can be used in a school.
- The school's Acceptable Use Policy (AUP) should take cognisance of the regulations regarding group broadcasts (e.g. video hire) and have steps in place to ensure compliance.

3. Books, newspapers and magazines

Description: Print (paper-based) material can take a number of forms but the most commonly used in a school are books, newspapers and magazines.

Uses:

- Print materials should be made available in schools because the curriculum is resource-based. Access to print material is essential if we are to create a literate society.
- Information-literate learners can only be developed if they have access to a range of resources, both digital and non-digital (paper based).
- One of the aims of education is to create discerning knowledge users who are ethical life-long users of information able to use a variety of resources.

Advantages:

- The advantage of print material is that it does not depend on electricity to be accessible nor expensive computer hardware which has to be maintained.
- Books go through an editorial and selection process so the information is, on the whole, trustworthy.
- Magazines can be used in a variety of teaching situations and the availability of paper-based material will encourage the reading habit as well as the fundamentals of information retrieval.
- Newspapers ensure currency of information and can also be used in a variety of ways for teaching e.g. debate topics.
- A range of resources encourages higher order thinking skills embedded in the research cycle e.g. comparison and evaluation.

Considerations:

- Print material needs to be managed, circulated and maintained.
- Theft, including vandalism is a key challenge to the provision of print material as well as the limitations of the size of the stock itself.
- If there is no budget or single person responsible for the collection, then this resource can be easily depleted or damaged.
- Books, newspapers and magazines date and thus require a budget to keep the collection current.

Recommendations:

- There should be a budget for paper-based material and the school should nominate an individual, in the absence of a school library/librarian to monitor and promote the use of the collection.
- Each school should ensure that key reference material that is current and relevant is available e.g. encyclopaedias, atlases and dictionaries.
- Credit should be given to the source of any information used for education purposes. Learners and teachers equally should respect copyright.
- Modifying work without permission can affect the reputation of the author. Permission should be sought.
- Photocopying of printed material should be limited to what is allowed in terms of the Copyright law.
- The school's Acceptable Use Policy (AUP) should take cognisance of the regulations regarding copyright and have steps in place to ensure compliance.
- Photocopying of printed material should be limited to what is allowed, and copyright respected

4. Online Computers and Mobile devices

Description: An online computer in this context is a fixed machine that receives and outputs data in a meaningful way and is connected to the Internet. It can be a standalone device or linked to other computers through a server but is designed to stay in one place. Mobile devices include any type of technology that is designed to be taken and used on the move. The term 'mobile technologies' often refers to tablets and cell-phones. It also applies to laptops and notebooks, media players and e-book readers.

The following is specific to mobile devices:

Uses:

Supporting learning in and outside the classroom through enhancing communications and access to information. There is an immediacy to the use of mobile devices i.e. 'anytime, anywhere learning' versus fixed technologies which are, at times, inaccessible.

Advantages:

- Parents/guardians can contact the learners during school hours and vice versa.
- The school can SMS the parents/guardians school information e.g. change of sport practice.
- Sharing information with others, such as showing class projects to parents or sending missed assignments to classmates that are absent.
- Use of cell-phones can contribute to securing a learner's own safety.
- There are many ways mobile devices, such as cell-phones, can support learning across various aspects of the curriculum. For example: in Visual Arts, learners can compare the quality and resolution of images taken on different devices in Life Orientation, learners can video and upload personal messages of support for safety campaigns, in Geography, they can investigate how topography affects mobile phone reception and plot data to GPS information systems.

- Giving learners flexible access to information, resources and tools; curriculum support e.g. social networking platforms, making learning a personal experience
- Recording and sharing experiences; and carrying out joint activities with learners from different schools or countries.
- Many cell-phones are equipped with calculators - plenty of new math curricula encourage the use of a calculator when problem-solving. A learner should become accustomed to having a calculator handy for both homework and real life maths applications.
- Many cell-phones are equipped with calendars – learners can be encouraged to load school events or project deadlines to their cell-phone calendars.
- Many cell-phones are equipped with a camera. These can be used for content creation, documentation and communication.
- If a learner is slow to copy notes from the board, pictures can be taken of the missed notes and accessed later. This also applies to sending notes to absent classmates.
- Sound recordings can be made of educational material.
- Interviews can be recorded with sound or video inserted into presentations and movies.
- As learners are using social networking platforms, teachers should be encouraged to add the contact names of his/her class to communication with the class collectively or individually on school related issues.

Considerations:

- Mobile devices have to be managed in an educationally sound manner as, by the very nature of their mobility, they can be very intrusive.
- Learners who carry mobile devices can be a target for thieves. Safety of learners on their way to and from school is a major consideration.
- Mobile devices can be used to cheat in exams by sending test questions to friends.
- The ability of mobile devices to make recordings, whether sound, picture or video, can be abused. For example:
- Recording individuals without their knowledge. Consent to being filmed or photographed should be specified in the school's Acceptable Use Policy (AUP).
- Recording illegal or inappropriate behaviour such as the abuse of people or animals for fun, bullying or taunting messages. Depending on the circumstances recordings can benefit as it is citizen policing. It is necessary nowadays and useful to record bad behaviour as proof of it. e.g. police brutality.
- Recording and sharing sexual behaviour – a practice called "sexting".
- Learners should never use mobile devices for illegal offences such as committing a crime, arranging a drug deal etc. and the penalties for such should be clearly specified in the school's Acceptable Use Policy (AUP).
- Mobile devices can blur the distinction between what happens at school, and outside of school. This can result in misunderstandings and confusion. For example – if a learner uses mobile devices to commit a crime at school this is taken to be the responsibility of the Safe School Committee and, if outside school, it is a matter for the parents/guardian and SAPS.

Recommendations:

- Outright banning of the use of mobile devices in a school can be self-defeating and educationally unsound. Furthermore the mobile device environment is becoming more and endemic and schools have a responsibility to manage it and educate around it. An Acceptable Use Policy (AUP) in a school should specify when and for what purpose the use of mobile devices is acceptable in a school and have steps in place to ensure compliance. This includes sending and receiving calls to/from parents/guardians.

The following is specific to computers and mobile devices

5. e-Mail:

Description: e-Mail, or electronic mail, is a method of exchanging digital messages across the Internet or other computer networks. This can be on a one-to-one basis or within a group, either open or closed.

Uses: e-Mail provides a quick and effective means of communication locally and internationally. It also allows for the attachment of documents and images which otherwise would have to be posted (snail mail) or faxed.

Advantages:

- e-Mail provides for a quick and simple response.
- It provides a useful record of communications leaving a 'mail trail' of evidence especially if "sent" items are never deleted.
- e-Mail gives time for a studied response to a discussion as opposed to the immediacy of a telephonic conversation or online synchronous (when things occur at the same time) communication e.g. chat room. Asynchronous (when things occur at unrelated times) communications allows for a period of time between responses.
- Unless e-mail is web-based, one need not be online to communicate; messages can be answered offline and only sent when connected.

- e-Mail is a useful way of sending attachments of text, images, sound or video.
- e-Mail can be sent to individuals or many, alternatively group mailing lists of recipients.

Considerations:

- e-Mail is subject to interception (violation of confidentiality, blocked delivery or replay), unauthorised modification of content or denial of message received. In other words, e-mail is exposed while in transit on the Internet.
- e-Mail fatigue is when there is an information overload and a user ignores a large number of e-mail messages after falling behind and failing to answer them.
- Sorting, sifting, filing and replying to e-mail can be time consuming with little benefit, especially if a user belongs to a number of mailing lists.
- Spam (group advertisements), flaming (insults) 'fun' mails (not work related), bogus virus warnings and untrimmed e-mails can all create problems for bandwidth, work concentration and time on task.
- Phishing and spoofing are bogus e-mails which take the user to websites which encourage the user to divulge sensitive information like PIN numbers. Victims can fall prey to this and be defrauded.
- Attachments can spread viruses and can also use up bandwidth unnecessarily. Users can be encouraged to use legal file sharing services like Dropbox, Google Drive, or Wetransfer instead.
- e-Mails can accidentally be sent to the wrong person or group or forwarded to a person who is not the intended recipient. They can also be copied either visibly or 'blindly' to an unintended recipient.
- To secure e-mail, one needs to ensure confidentiality of the message, message integrity (what the receiver sees is exactly what was sent), non-repudiation (the sender cannot deny that the message was sent) and authenticity of the sender (the sender is who the sender claims to be).

Recommendations:

- Users must be made aware that they will be held responsible for the content of any e-mail message they transmit.
- e-Mail should not contain messages using language or content that is inappropriate or unacceptable.
- Users should be made aware of basic rules of Netiquette e.g. the use of all capitalised words is considered shouting.
- The immediacy of the medium must be managed; users should avoid a hasty reaction to an e-mail if emotionally charged.
- Users should be taught the importance of not divulging passwords, e.g. via email, and also logging off after use.
- Teachers and learners should understand what spam is, including hoaxes, and not forward such messages, contributing to unnecessary use of bandwidth. Users should be educated on what type of e-mail to ignore or delete. Specific examples include 419 scams, phishing/banking scams, and so on.
- e-Mail users should take note of the size of attachments and reduce the file size where possible e.g. converting images to .jpg format or zipping files, or using a free file sharing service such as Dropbox, Google Drive, or Wetransfer At present, any attachment over 3-4 MB is considered excessive.
- All e-mail should have relevant subject lines and follow a thread of discussion.
- To mitigate the risks associated with the use of e-mail, users should be educated about security and personal risks associated with the use thereof.
- An Acceptable Use Policy (AUP) in a school should specify when and what purpose the use of e-mail is acceptable and have steps in place to ensure compliance.

6. Web sites (World Wide Web)

Description: The World Wide Web, is a global set of interconnected computer websites using a protocol which allows them to connect to each other via links. It provides a platform for a massive library of current, relevant and pertinent information in a variety of formats.

Uses: The main goal of Internet access in education is to enrich and extend learning through access to information, also enhance communications and sharing. Collaboration in the online environment allows both teachers and learners to be global citizens through being able to quickly and easily communicate across the world as well as developing their skills for the 21st century.

Advantages:

- Access to a range of resources in the education environment as well as generally.
- Access to current information and the ability to keep track of rapidly changing situations – an advantage over print material which can be slow and expensive to update (excluding newspapers).
- The ability to communicate with others in online forums and other social networks. Such communication is not limited to the purely social, but can be used to support professional development as well as lifelong learning.
- The opportunity to broadcast opinions and information in the form of articles published on blogs and other websites.
- Sharing of teacher developed resources that have been peer reviewed, or with websites that have been evaluated by the education community,
- The opportunity to build lifelong research skills.
- The ability to interact with people from all over the world and be exposed to new points of view, alternative perspectives and other cultures (Communities of Practice – COP's).

Considerations:

- Anybody can create a website and upload information either true or not, unlike a traditional library whereby books go through an editorial and selection process thus ensuring a measure of quality control.
- Inappropriate material can be accessed online very easily, both deliberately as well as inadvertently. Users need to be aware that their use can be monitored and they can be identified for inappropriate use. Users of the Internet create a digital trail which cannot be erased.
- Creating White Lists, or pre-screened lists of Internet sites, is appropriate in some instances but it must be remembered that learners must be educated to manage the Internet even when away from the protected environment of a school. Furthermore, even if one creates a page with a whitelist of acceptable sites, there's nothing to say that deep within one of those sites, there will not be a link outside of the whitelist, which takes the user to a site which is not on the whitelist, and potentially problematic.
- Digital literacy, i.e. the ability to find, discern, select and use online information appropriately is a skill that needs to be taught. If learners do not understand that much of the information on the Internet is opinion, not fact, they will be the victims of misinformation.
- Modifying work without permission can affect the reputation of the author. Permission should be sought. If the material is marked as Creative Commons, this still applies.
- There is an erroneous assumption that digital resources carry more credibility. The opposite is the case.
- Misuse of access to the Internet can cost the school both bandwidth as well as working time on the part of both learners and teachers.

Recommendations:

- All schools should have an information literacy plan in place whereby learners and teachers are taught how to find, evaluate and use the range of information resources available.
- All methods which limit access – whether lists of suitable sites, lists of blocked sites, or lists of unsuitable words, should be developed with the input of teachers who will be affected. These lists can be used by various technologies to inhibit access.
- Careful thought should be given to the process whereby these lists and limitations are managed and adjusted so that they do not adversely affect the ability of teachers to teach or learners to learn.
- The content of web pages or web searches can be filtered for unsuitable words using forensic software or firewalls, but care should be taken these do not impact on legitimate use. For example, blocking the word “breast” would make it impossible for anyone to find information on “breast cancer”.
- White lists or pre-screened internet sites can be uploaded onto a school server.
- Shortcuts to useful, interesting and popular sites that are appropriate to the learner’s age can be placed on the desktop of each computer.
- Browsers come with built-in safety parental control features; parents/ guardians can protect the computers in the home through using these.
- Having computer screens in public place minimises the temptation to misuse access as the user’s activities can be directly observed.
- Software can be installed so that all computers are “set to default” each morning. This will delete unauthorised material from the computers. An example of this kind of software is DeepFreeze.
- Applying rating settings on browsers, checking the history (visited sites) in the browser and password protecting computers are all measures which can be taken.

- Checking the history of sites visited can be a useful tool in managing user access and misuse.
- Making sure that learners know that their use is monitored and that they have to take responsibility for how they use the Internet.
- Phishing and spoof sites. To avoid these dangers, users are advised to:
    - Log off after using a site especially on a public computer as found in an Internet Café or school computer room,
    - Avoid clicking a URL link in an email
    - Check for a padlock in the address bar of the browser if it is a financial site
    - Look for the “https” in the site address, versus “http” which is insecure
    - Change passwords and PIN numbers regularly.
    - Check that the URL matches the company name, e.g. that banking site URLs match the bank’s name.
- An Acceptable Use Policy (AUP) needs to be in place and have steps in place to ensure compliance in order that users accept their responsibility for their use of the Internet

7. Social Media and Social Networking

Description: Social Media: refers to the platforms that make it possible for users to actively participate online by creating their own online presence, and communicating with others. User-created communication and content that may take the form of video, audio, text or multimedia that is published and shared in a social environment, such as a blog, wiki, forum, podcast, social bookmarking or video hosting site. Access can be either on using an online computer or using mobile devices such as cell-phones.

Social Networking: online platforms that provide means of personal communications between participants such as FaceBook, LinkedIn, Twitter, WhatsApp, and many others

Uses:

- Participating in online communities that share an interest – to gain or share knowledge.
- When used positively the social media platforms allow people to share music, art, video, opinion, collaborate on work or have discussions and learn from one another.
- Socialising: keeping in touch with existing friends and finding new friends. A channel for the promotion of a cause or product.
- Social media platforms allow users to link up with each other quickly and effectively. This can be particularly effective in the professional environment.
- Individuals can use social media to further their personal or professional goals e.g.
    - Creating and managing their online presence to form an impressive online CV
    - Communicating their opinions, values, and experiences
- Sharing information, pictures, activities, resources and websites can assist lifelong learning and create Communities of Practice (CoPs).

Advantages:

- There can be opportunity for substantial professional growth as members of the group are kept abreast of the latest developments and the views of thought leaders.
- Users can create an impressive online presence to further their professional goals – for example, writing a blog in the area you specialise in to prove your expertise.

- A way of connecting and reconnecting with people.
- Users of these social media platforms have the ability to create their own material and post whatever they like in the platform of their choice e.g. films, magazines or text.
- When used positively the social media platforms allow people to share music, art, video, opinion, collaborate on work or have discussions and learn from one another.

Considerations:

- As with all online communication tools the social media environment has to be managed so that it does not become all-consuming.
- Cognisance must be given to Copyright law when sharing these media.
- Modifying work without permission can affect the reputation of the author. Permission should be sought.
- Like e-mail etc, issues of privacy and circumspection apply as any communication can be forwarded and very often credit is not given to the source.
- Social media networks are often visible to people from the user's professional as well as personal life. This blurring of social and professional lines can result in embarrassing or otherwise inappropriate revelations. For example – if a teacher "friends" learners on Facebook, they should be aware of what aspects of their profile are visible to the learners.
- Online stalking, harassment and bullying can occur, with resulting emotional stress.
- Naive users may fall prey to hackers, phishers and other online scams.
- Users should take care to familiarise themselves with the privacy settings, and avoid sharing any information that they don't wish to be publicly available.

- Users should take care not to share compromising images or inappropriate messages that may damage their reputations later in life (creating a digital footprint).
- Users should be aware that behaviour on sites may or may not be moderated, and content is usually uncensored.
- Social networking platforms can be bandwidth intensive.

Recommendations:

- Activity is advised to further professional development and interaction in the education environment.
- Learners should be taught critical thinking skills and digital literacy to enable them to navigate safely through this online world.
- Social networking sites offer a variety of privacy settings and again, circumspect use of these sites is advised.
- Learners should be sensitised to the appropriate etiquette for each online environment, and be made aware of the consequences of misbehaviour.
- Learners should be made aware of the consequences of their use of social media, and encouraged to act responsibly.
- An Acceptable Use Policy (AUP) in a school should specify when and for what purposes the use of social media platforms are acceptable in a school.

8. Online gaming

Description:

An online game is a game played over some form of computer network. Online games can range from simple text based games to games incorporating complex graphics and virtual worlds populated by many players simultaneously. Many online games have associated online communities, making online games a form of social activity beyond single player games.

Uses: These can be educational e.g. Teen Second Life ages 13-17 whereby learners create "avatars," or online personas, which can explore, meet other residents, socialise, participate in individual and group activities, and create and trade virtual property and services with one another, or travel throughout the world (which residents refer to as "the grid"). Epistemic games offer an opportunity to build bridges between theory and practice. These games could also afford learners the opportunity to see what it is like being a scientist or doctor, etc.

Advantages:

- Developing computer skills and interacting online.
- Learning in a fun and interactive way.
- Developing social and problem skills in a more contextualised environment.
- Learning 21st century skills.

Disadvantages:

- Can form addictive behaviour and also impact on social behaviour especially if content is particularly violent/sexual in nature.
- Games, particularly games that aim to teach and not simply entertain are difficult to design and develop.
- Developing games are expensive and time-consuming.
- Online gaming can also be a drain on networking resources.

Recommendations:

- Games should have clear educational goals.
- Games need to be developed that provide learners with a safe environment in which to learn and explore.
- We need to not only educate our learners in using technology but also how to use it ethically and responsibly.
- Develop epistemic games to embody professional occupations and help learners learn these cultures that define their community of practice (CoPs).
- Games can help prepare learners for a global world, of dynamic change and possibility.
- An Acceptable Use Policy (AUP) in a school should specify when and what purposes the participation in online gaming is acceptable in a school.

Published by the Department of Basic Education

222 Struben Street

Private Bag X895, Pretoria, 0001

Telephone: 012 357 3000 Fax: 012 323 0601

ISBN: 000-0-0000-0000-0

© Department of Basic Education

website	facebook	twitter
www.education.gov.za	www.facebook.com/BasicEd	www.twitter.com/dbe_sa