SPRINGVALE PRIMARY SCHOOL

Established 1981



ICT POLICY

REDRAFTED: 2016 REVIEW: 2018

DOCUMENT CONTROL

DOCUMENT DETAILS

ITEM	VALUE		
Amendments Requested By:	School Governing Body		
Document Revision Date:	May 2016		
Author/s:	SGB		
Security Level:	Confidential		
This copy printed on:	09/11/2018		
Document Name:	SGB – ICT Policy		

REVISION CONTROL

REVISION	DATED	REVISED BY	DESCRIPTION OF MAJOR CHANGES
1	2007		
2	2008		
3	2010		
4	2012		
5	2016	SGB	Formatting

SIGNATORIES

Principal

N. Vallabh

SGB Chairperson

M. Bowker

SGB Treasurer

K. Kambule

SGB Vice Chairperson

Table of Contents

DO	OCUMENT CONTROL					
Tab	able of Contents					
1.	PREAMBLE					
2.	PURPOSE					
3.	D	EFINITIONS AND ACRONYMS4	1			
4.	Α	PPLICATION AND SCOPE OF THE POLICY4	1			
5.	LI	EGISLATIVE FRAMEWORK5	5			
6.	R	ELEVANT POLICIES AND PROVINCIAL CIRCULARS5	5			
7.	Ρ	OLICY STATEMENTS	5			
8.	R	ULES FOR THE USE OF COMPUTER LABORATORIES12	2			
9.	Α	CCEPTABLE USE OF INTERNET AND EMAIL	3			
9	.1	School owns user email	3			
9	2	Acceptable use	3			
9	3	Unacceptable use	1			
9	9.4 Safety and security of users					
10.	0. POLICY ON CYBERBULLYING					
11.	1. CELLULAR PHONE					
INA	ANNEXURE A19					
ANI	ANNEXURE B					
ANI	ANNEXURE C. 22					

1. PREAMBLE

Springvale recognises that today's world is increasingly driven by technology and information and that preparing learners for success in adult life demands that we equip them with the necessary skills. It also means that school management and administration systems need to reflect the world we live in and match the level of usage of technology that is becoming the accepted norm for organisations across the world.

The school will encourage the appropriate use of ICTs where it believes that such use will improve efficiencies and educational outcomes.

The school will therefore make full use of its current ICT resources, and will make provision for maintenance and acquisition of ICTs as well as increased utilisation of ICTs in its development plan and in the school budget. Priorities will be identified on an annual basis, and evaluated and updated quarterly to ensure that goals are achieved.

A system will be applied to ensure that ICTs are used optimally. This will include a timetable for the use of the school computer laboratory and an asset management and booking system for all other items.

The school will encourage community involvement in its use of ICTs in the school. It will keep parents, local businesses and other community members informed of progress and usage and will request technical and professional assistance as well as donations and sponsorships where parents and other community members are able to provide these.

2. PURPOSE

The purpose of this policy is to outline the school's approach to the use of ICTs for management, administration, teaching and learning in the school. It will be used

- To ensure all staff understand and agree on the approach to ICT
- To assist planning and promote development
- To explain the school's position to outsiders, including parents
- To assist the school management in the allocation of funds

3. DEFINITIONS AND ACRONYMS

ICT: Term used to include devices such as computers, tablets, digital cameras, TVs, video or CD players, CDs, MP3 players, overhead and data projectors, electronic whiteboards, cell phones, memory devices and printers. It also includes programmes or software that can be used with the equipment, as well as the use of email and internet services and utilisation of computer laboratories

SMT: School Management Team

SGB: School Governing Body

4. APPLICATION AND SCOPE OF THE POLICY

This policy applies to the SMT, teachers, administrative staff and learners.

5. LEGISLATIVE FRAMEWORK

This policy is written within the framework of the following Acts that pertain to education in South Africa:

- RSA Constitution Act 108 of 1996 as amended
- School Education Act of 1995
- South African Schools Act 84 of 1996 as amended

6. RELEVANT POLICIES AND PROVINCIAL CIRCULARS

This policy should also be read in conjunction with the following Provincial or internal school circulars, policies and procedures:

- Disciplinary policy
- Asset management policy
- Emergency procedures
- Acceptable use for internet and web usage policy
- Procedures for the removal of school equipment from school property
- Rules for use of the school Laboratory
- Cell phones for learners policy
- Gauteng on Line Code of Ethics and Conduct, Circular 13/2004, 24 February 2004

7. POLICY STATEMENTS

7.1 Goals for ICT usage in the school

According to the 2009 SAIDE benchmark7, the school scored an overall 41% for e-Readiness. The goal of the school is to regard this score as the baseline and to improve against it on an annual basis. Details will be included in the annual school development plan.

The baseline scores are as follows:

No	Item	ldeal Score	School score	Comment
1	Mins per learner per computer per day	40 mins (Primary school)	0	Particular attention will be given to ensuring that learners have access to ICTs, especially the computer laboratory, and a timetable will be set up to prioritise usage
2	Mins per teacher per computer per day	160	54	There is very little usage by teachers. Priority will be given to acquiring additional computers that will be available to teachers for administrative tasks and for preparation for lessons. Teachers will be encouraged to acquire their own laptops if possible. In addition, certain classes and subjects will be prioritised to ensure that teachers start using the computer laboratory for teaching and learning

No	Item	Ideal Score	School score	Comment
3	Mins per admin staff per computer per day	420	630	Good usage by admin staff. The focus will be on increasing the number of administrative tasks to be completed electronically. Admin staff will also be scheduled to assist teachers with their administrative and preparation tasks
4	School has an ICT co- ordinator	1	1	Roles will be clarified and the focus for the Co-Ordinator will be optimal use of the computer laboratory and hands-on assistance to teachers when required
5	School has an ICT policy / plan	1	1	Review and update annually
6	School has at least 1 printer	1	1	Consider acquiring additional printers for the computer laboratory so that learners and teachers can print out their work. School budget should include printer cartridges and paper, and provision for maintenance
7	Frequency of internet connectivity	Above 75% = 1	0	This is a major area of concern and attention will be given to making contact with the Help Desk and to following up on poor service if necessary. We will call on the services of the District IT Support Technicians to assist and will also book the mobile computer laboratories when necessary
8	Teacher confidence	2	0.6	Most teachers have had basic computer literacy training. The focus will be on providing resources to allow them to practice their skills – this is for use of computers as well as other ICTs such as data projectors, TVs, CDs, etc. Assistance will be provided from the ICT Co-Ordinator, the District IT Support Technicians and from training modules available online and on the laboratory server. Teachers who have not had training for basic computer literacy will be scheduled to attend courses for this. Teachers will attend additional training courses where this will assist them in making use of ICTs for administration and/or teaching.
9	Learner access to computers outside class	3	0	The computer laboratory will be open after school for extra-mural English and mathematics, or by arrangement with the teacher. Teachers will be allocated to supervise during these times
10	SMT use of ICT	1	1	The SMT is currently making good use of available computers for management reports, timetabling and school records. The goal is for all correspondence and reporting to the District to be electronic.

Springvale Primary School – ICT Policy
The information contained within this document is confidential and for the exclusive use of Springvale Primary School

7.2 The use of ICTs in teaching and learning

	Teacher usage of	ICTs	
Admin	Prep	Teaching	Learning
0%	15%	9%	4%

- Teachers will be expected to make use of the training that has already been provided and to improve their own skills in the use of ICTs for administration, lesson preparation and for teaching, and the school will encourage them to do so and assist through training programmes where possible and through making ICTs available and accessible.
- Teachers who are eligible for laptops and cell phones in terms of GDE policy will be encouraged to make use of the facilities provided.
- Required teacher skills include basic computer literacy (i.e. the ability to use the MS
 Office suite of Word, Excel and PowerPoint and the ability to access the internet and
 use email) as well as skills in the usage of other equipment such as data projectors,
 TVs, DVD's and CD players, etc.
- They will also be expected to learn how to use educational programmes and systems
 that are acquired by the school or that are available through the GDE central database
 or other sources, where such usage is appropriate to the subject matter and where it
 will benefit learner progress.
- Part of classroom assessment of teachers will include an evaluation of their use of available ICTs for teaching and learning.
- The school standard is that examination papers, worksheets and assessment reports will be typed where this is appropriate.
- It is school policy that all learners will have access to ICTs and that they develop at least the basic computer literacy that would be associated with their grade.
- Where resources are limited, the school will set the rules to prioritise usage.
- Usage of school computer laboratories will be governed by timetables during school hours, but will be available for individual learners or groups of learners to use after school.
- Teachers will be allocated to supervise during these times and until closing time at 15:00.
- The school will give attention to learners who have special educational needs, both to
 accommodate those with physical disabilities (e.g. utilising special spaces in
 laboratories for learners in wheelchairs) as well as accessing specialised software and
 equipment for those with learning disabilities, providing such acquisitions are approved
 in the school budgeting process or they can be obtained through donations or
 partnerships.

7.3 The use of ICTs for management and administration

- Springvale Primary School will provide Personal Computers (PCs) primarily for the use
 of SMT members. Where these PCs are not being used by SMT members they may
 also be used by other teachers for administrative and preparation purposes.
- All school staff members, including administrators, teachers and SMT members will have an email address and will be able to send and receive e-mails.
- School administrative staff will allocate a certain number of hours per week (to be agreed on an individual basis depending on other workloads) to assist teachers by typing material, capturing data, and preparing presentations, worksheets and reports. Requests for such assistance should follow normal school procedures and be submitted via agreed channels and within agreed timeframes.
- Where appropriate, all school records will be produced and stored electronically and on hardcopy format e.g. Retention Schedules. This includes such items as learner records and reports, minutes of meetings, financial records, school development plans, reports and management information submitted to District and/or Provincial level, etc.
- Official communication with parents, SGB and other community members and the GDE will be electronic where possible. This includes the use of email and SMS services.
- A protocol for backup of this data and for protection of confidentiality and privacy will be drawn up and communicated to all relevant staff members.

7.4 Training and development of teachers, administrative staff, SMT members and SGB in ICT usage

- Training in ICTs will be added to the schedule of training for staff members and SGB members. This will include attendance at in-service and formal training provided by the Province to improve skills in ICT usage.
- In addition, the school will investigate other ways of providing training to staff members, including appointing an ICT Co-Ordinator with sufficient skills to be able to assist other staff members, making use of District officials with sufficient skills to be able to assist staff members, making use of interns that have been deployed to the district or the school, encouraging staff members to help each other and requesting community members, including parents, with sufficient skills to assist. Specialised or advanced training supplied by external or private companies will only be considered under exceptional circumstances.
- The school also expects staff members to take personal responsibility for their own development through practising skills that they have acquired during formal training

programmes, requesting help from others and self-training via online professional development modules.

- The school computer laboratory will be open in the afternoons according to arrangement and extra mural programme. Teachers will be permitted to take home specific items for practice and preparation of lessons with the necessary arrangement and approval (e.g. cameras and video equipment, laptops, recording equipment, etc) subject to availability and the following of procedures relating to removing school property from the premises.
- Inappropriate use of school resources, such as using class time to surf the web for personal purposes or allowing unauthorised people to use school equipment, will be dealt with in terms of school disciplinary policy.

7.5 Management of hardware and software

- All ICTs will be added to the school's asset register and will be insured.
- The school will strictly enforce licensing agreements for software and will not allow the loading of illegal software onto any school computers.
- Where new hardware and software is to be acquired, cognisance will be taken of the need for compatibility with existing equipment and of any requirements or conditions put in place by the GDE.
- All ICTs should be handled with care and treated responsibly. Separate procedures
 will be set up where required to cover specific requirements, but in general it can be
 said that staff and learners should keep equipment clean and adhere to suppliers'
 instructions for use. Any deliberate or malicious damage to property will be dealt with
 in terms of the school's disciplinary policy.
- A booking and tracking system will be set up to ensure that ICTs can be allocated to specific staff members or others and can be tracked. A separate procedure will be drawn up to set out the steps to be followed and to cover issues such as insurance and the process to be followed in the event of loss or damage to equipment.
- The computer laboratory will be locked when not in use and at the end of the school
 day and the key will be kept by the relevant members of staff. All portable items such
 as laptops, cameras, data projectors, printers, CD or MP3 players should be locked
 away securely when not in use, either in the responsible teacher's storeroom or in the
 central storeroom.

7.6 Data Management

Anti-virus and anti-hacking software and mechanisms will be installed and maintained by the school and specific rules will be put in place to ensure that viruses are not transferred to school computers by foreign devices such as personal memory sticks or CDs. Should anyone wish to

use a personal device, then it is a requirement that they first run an anti-virus check on it before commencement of work with it.

The school will be vigilant in matters relating to:

- copyright, intellectual property and piracy
- plagiarism ensuring that teachers and learners acknowledge the source of information
- confidentiality and protection of privacy, including usernames, emails, files and documents such as learner records, examination papers, etc
- learner safety, including ensuring that there is no access to pornographic or other unsuitable sites and that learners are made aware of the potential dangers of providing personal details on the web
- providing a firewall service to control internet access
- use of personal web-enabled cell phones or 3G cards to access or display data or pictures

7.7 Planning and budgeting for ICTS

- 7.7.1 ICTs will be added to the school planning and budgeting systems to ensure ongoing usage and maintenance of current assets as well the acquisition of new hardware, software and skills.
- 7.7.2 Depending on priorities for the year, a portion of the budget for the school budget will be allocated to ICTs.
- 7.7.3 The first priority for the use of these funds will be to maintain the current resources and to ensure that they can be used optimally. This will include provision for basic items such as print cartridges and printing paper for use in computer laboratories and for the provision of typed worksheets and other documents for teaching and learning purposes, payment for connectivity to ensure access to the internet, payment for maintenance of equipment in the event of damage or wear. Next priorities will be established on an annual basis and monitored and updated every quarter.
- 7.7.4 In addition, the school will ensure that it keeps itself up to date regarding what is available and will be paid for by the GDE (. The school will also actively set up fundraising projects and will seek partnerships with local businesses and other enterprises to increase the funding it has available for ICTs.

Elements to be included in the budget are:

- Maintenance of equipment
- Printing costs

Springvale Primary School - ICT Policy

The information contained within this document is confidential and for the exclusive use of Springvale Primary School

- Connectivity
- Hardware
- Software
- Technical support
- Insurance
- Staff development

7.8 Roles and responsibilities

The final responsibility for ensuring that ICTs are used effectively in the school lies with the Principal and the SMT. To assist in the task, the school will appoint an ICT Committee and at least one ICT Co-Ordinator (an additional Co-Ordinator will be appointed if necessary to share workload). The ICT Co-Ordinator/s will be selected primarily on the basis of technical expertise and management ability. Roles will be as follows:

7.8.1 School ICT Committee

- ICT planning for the school
- Working with the SMT to develop and implement ICT policies for the school
- Scheduling and monitoring training
- Identifying, evaluating and selecting educational software
- Representing the school in all e-Learning activities at District or Cluster level or at ICT forums
- Promoting ICT integration in teaching and learning, by
 - o Assisting teachers with lesson plans
 - o Informing teachers of tools and materials that are available
 - Recommending appropriate ICT tools for particular teaching and learning purposes
 - Monitoring and evaluating the effectiveness of ICT use in the school, incl.
 - Attendance at training programmes
 - Access to computers for teachers and learners
 - Use of ICTs for administrative and management purposes
 - Levels of computer literacy SMT, SGB, teachers, learners
 - Extent of integration of ICTs into teaching and learning (incl CDs, DVDs, TV, etc)
 - Implementation of timetabling plans
 - Meeting provincial priorities

7.8.2 ICT Coordinator/s

The ICT coordinators will be responsible for;

- Providing technical assistance
- Providing training for learners
- Troubleshooting when there are system or equipment problems
- Reporting and following up on broken or faulty equipment or systems

Springvale Primary School - ICT Policy

The information contained within this document is confidential and for the exclusive use of Springvale Primary School

Dated: April 2016 Revision: 1.0

- Managing the computer laboratory, including timetabling
- Informal use of the computer laboratories outside of school hours
- Enforcement of the rules around use of equipment, virus protection, internet usage, etc
- Managing other ICTs in the school, including overseeing asset registers
- Booking arrangements for teachers to use equipment and facilities
- Providing on-site user support
- Assisting learners, teachers and administrative staff with technical queries
- Assisting teachers to develop documents or resources for their lessons
- Providing training for teachers and administrative staff in using ICTs
- On request / in response to technical queries (e.g. on usage of packages such as MS word or excel, use of cameras, data projectors, etc)

8. RULES FOR THE USE OF COMPUTER LABORATORIES

The rules for the use of computer laboratories are;

- During class time the laboratory will be used for classes according to the timetable
- The laboratory will be open during school hours until 15:00
- Learners and teachers may book time to use the laboratory during these times
- No learners may be in the laboratory without the supervision of a teacher or other responsible person
- Strictly no food or liquids are allowed in the laboratory
- The laboratory is to be kept clean at all times and must be neatened up by learners after lessons
- No items may be removed from the laboratory without permission
- The room temperature should be about 22°C. If the weather is hot, keep the door and windows closed and the air conditioners switched on.
- Learners must not tamper with computer systems, printers, other hardware and equipment without having permission to do so
- No learners may load programmes or software onto the computers or link any hardware to the network without the permission of
- Learners may not link to the internet via an unauthorised service provider. Neither may
 they operate another email account (e.g. Hotmail or web-based email) from the
 network
- Learners will use the computers for learning purposes. Playing games or browsing the internet will only be allowed if you have been given permission to do so
- Learners must respect the rights of others and obey the general rules relating to use of computers and the internet
- Learners must get the permission to store data and files
- Learners may not delete, rename or damage the files of others
- Learners may only use their own login account and files. Using someone else's without permission will be regarded as theft

- Writing an e-mail message whilst masquerading as another person is a very offensive form of fraud
- Learners must not deliberately annoy others and invade their privacy, e.g. through reading other people's mails or files without permission, sending or making accessible obscene, abusive or threatening messages, or flooding a person's account with multiple emails
- Accessing, downloading, uploading, saving, receiving or sending material that includes pornography, vulgar, sexist, racist, threatening, violent or defamatory language or material is strictly prohibited and is regarded as a violation of the internet
- Learners may not forward "junk mail" and create or forward chain letter e-mail
- Any intentional damage to physical property (computers, printers, desks, etc) as well as damage to information not belonging to you and intentional misuse of system resources will be regarded as vandalism. This includes deliberately introducing codes and programmes that will damage or hinder the performance of any computer (computer viruses, bugs and worms, Trojan horses, etc)
- For safety and security reasons, learners should not provide personal information, including passwords, email addresses on bulletin boards, chat rooms or other services, just as they would never give their address to a stranger
- Please note that the principal or other authorised person may access your emails, files and record of internet sites visited if they believe it is necessary to do so

Violation of these rules may result in disciplinary action, including suspension of computer rights

9. ACCEPTABLE USE OF INTERNET AND EMAIL

These conditions apply to learners, teachers and administrators who make use of school computers and other electronic equipment to access the internet and emails and also to those who use their own web- enabled cell phones or 3G cards and can access internet sites at the school or while on school business.

9.1 School owns user email

All users should respect the privacy of files and email messages, and no-one should read personal mail unless permission has been given to do so. However, the school owns any communication sent via email or that is stored on school equipment. Management and other authorised staff have the right to access and control any material in individual user emails or on school computers at any time.

9.2 Acceptable use

Voice mail, email, and internet usage assigned to school computers or telephone extensions are for the purpose of conducting school business. Access to the Internet is specifically limited to activities in support of official school business, including educational and research purposes.

Private use of such equipment or resources is permitted to the extent that;

It is not excessive

- If by a staff member it does not interfere with the performance of his or her duties as a staff member
- It does not impair the rights of other members of the school community

Software needed, in addition to software provided by the school and the GDE, must be authorised by the principal and the ICT Committee, who will follow the procedures required by the school and the GDE regarding acquisition of software.

If any user has a question regarding acceptable use he/she should check with the responsible teacher or the ICT Coordinator for additional guidance.

9.3 Unacceptable use

Internet access via computer or any other electronic device shall not be used for any illegal or unlawful purposes. Examples include

- Viewing, storing, downloading or forwarding defrauding, violent, threatening, harassing (race, gender, nationality, religion, etc), defamatory, pornographic or obscene materials
- Bullying others ("cyberbullying") see Appendix 1 for examples of this
- Impersonating another user or another person
- Damaging or deleting files of another user
- Obtaining access codes and/or passwords of another user without authorization
- Sending bulk unsolicited mail, mail-flooding, or excessive cross postings on newsgroups (called spam)

School email or messaging services shall not be used to harass, intimidate or otherwise annoy another person. It should also not be used for private, recreational or other non-school related activities including commercial or partisan political purposes or for personal gain, if this has not been authorised.

Users shall not attempt to circumvent or subvert security measures on either the school's network or any other system connected to or accessible through the Internet. Any form of hacking is specifically forbidden.

Users may not make or use illegal copies of copyrighted material, store such copies on school equipment, or transmit these copies over the school network.

Loading of illegal software (i.e. software that the school has not purchased or does not have a licence for) directly onto school computers or downloading of illegal software via the internet, including music and film material is strictly forbidden. Likewise, users may not illegally copy, change or transfer any software provided by the school and GDE.

9.4 Safety and security of users

9.4.1 Child safety on the internet

Of particular concern in the school environment is exposure of learners to online predators i.e. adult internet users who exploit vulnerable children or teens, usually for sexual or other abusive purposes and who cause learners distress, fear or embarrassment.

Rules to ensure child safety on the internet will be strictly enforced. These rules and the rationale behind them will be explicitly taught to learners as part of the process of teaching them to use the internet and will be prominently displayed on the walls of computer laboratories and in other venues where learners may have access to the internet. The rules will include those already listed as part of acceptable and unacceptable usage, and will also include the following rules;

- Learners may not divulge personal information which could be used to locate or identify them
- If a school has a website, care should be taken to protect the identities and personal details of learners who may be featured on the site for achievement and other reasons
- Regular checks will be run to monitor sites being accessed by learners
- When sending mass emails to parents use bcc (blind copy) so that parent email addresses are not made public

9.4.2 Breaches of confidentiality and security

Internet use brings the possibility of breaches to the security of confidential school information. Spy ware allows unauthorized people, outside the school, potential access to school passwords and other confidential information. The school may also be subjected to phishing which is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and banking details by masquerading as a trustworthy entity. Internet use also creates the possibility of contamination to the school system via viruses.

Some measures to ensure confidentiality and security include

- The school will ensure that it maintains a firewall and anti-virus system as part of the general setup in the school. It will also set up its own white and black lists for internet browsing. If required, the school will consider acquiring proprietary software which can be updated daily to control internet connectivity per user/group.
- Users may not use own memory sticks/flash drives or CD's and DVDs in school equipment, unless this has been authorized and they have run a virus check on these devices prior to using them on school equipment.
- School memory sticks, CDs, etc are not to be used in privately owned PCs and laptops, unless this has been authorized and the privately owned PC or laptop has been certified by the school as having the appropriate anti-virus and anti-spy ware protection.
- Users may not connect a PC to the school network without running virus detection software.
- School confidential information must not be shared outside of the school, without authorisation, at any time

Violations of this policy will be handled in accordance with procedures established for staff or student discipline.

10. POLICY ON CYBERBULLYING

The following actions are considered as Cyberbullying and any instance of cyberbullying will be dealt with severely in line with the disciplinary policy on serious contraventions.

Some of the actions mentioned below may be considered as criminal offences and may lead to reporting to the South African Police Service.

Some of the instances below as identified may relate to compulsory reporting to the SAPS

Actions in terms of this policy will not preclude any parent from reporting the matter to the SAPS

10.1 Instant Messaging/Text Messaging Harassment

- Sending of hateful or threatening messages to other learners
- Warning wars: Many Internet Service Providers offer a way of "telling on" a user who
 is saying inappropriate things. Learners often engage in "warning wars" which can lead
 to someone being suspended or "offline" for a period of time. While this should be a
 security tool, learners sometimes use the Warn button as a game or prank.
- Text wars or text attacks when learners gang up on the victim, sending thousands of text- messages to the victim's cell phone or other mobile device.
- Creating a screen name that is very similar to another learner's name and then use this name to say inappropriate things to other users while posing as the other person.

10.2 Stealing passwords

Stealing of another learner's password and chatting to other people, pretending to be the other learner is a criminal offence as well as using another learner's password to change his profile to include sexual, racist, and inappropriate things that may attract unwanted attention or offend people.

10.3 Blogs

Using of blogs to damage other learners' reputations or invade their privacy.

10.4 Web sites

The creation and/or use of Web sites that may insult or endanger others.

10.5 Sending Pictures through E-mail and Cell Phones

Sending of mass e-mails to other users that include degrading pictures of other learners. Sending of pictures that contain illicit or inappropriate content (including of pornographic nature). Children must be made aware of the fact that any picture of a naked person or body part or action of a sexual nature may be considered to be pornography.

10.6 Internet Polling

"Who's Hot? Who's Not?" These types of questions run rampant on Internet polls, created by learners and other teens. Such questions are often very offensive and hurtful.

10.7 Impersonation

Posing as the victim or posting provocative message in a hate group's chatroom, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier. Sending a message to someone posing as the victim, saying hateful or threatening things while masquerading as the victim. Altering a message really from the victim, making it appear that they have said nasty things or shared secrets with others.

11. CELLULAR PHONE

Springvale does not permit the use of Cellular Phones during school time.

- 11.1 Some concerns that may be associated with learners having cellular telephones include the following:
 - Learners who carry or use cell phones (including head phones) in public, particularly when travelling to and from school, have become the targets of criminals
 - Theft of cell phones at school from bags and blazers is a persistent problem
 - Some learners are sometimes careless with their cell phones and leave them lying around or in blazers and bags which are left unattended. Lost and mislaid cell phones are frequently claimed to be stolen when this is not the case
 - Learners are distracted from their work by the phones
 - Cell phones may carry private and personal material, including photographs, video clips, voice messages and personal details which may become accessible by undesirable individuals and groups when cell phones are lost, borrowed or stolen.
 - Cell phones can be used for cheating in examinations
- 11.2 The following rules will be applied to learners bringing cell phones to school:
 - The school will not take any responsibility whatsoever for a cell phone which is lost or stolen, no matter what the circumstances. This includes the loss or theft of cell phones that may be handed in to teachers and or coaches for safekeeping, as well as to cell phones which have been confiscated from students who use them in defiance of the school rules
 - Cell phones must be switched off (not "on silent") during the school day other than during official break periods
 - Cell phones may under no circumstances be brought into examination venues
 - If a learner is found using a phone when not permitted to do so, the phone will be confiscated until the end of term

Springvale Primary School - ICT Policy

The information contained within this document is confidential and for the exclusive use of Springvale Primary School

Dated: April 2016 Revision: 1.0

- Learners found with any pornography or any other distasteful material on their phones will be dealt with severely and parents will be informed
- Learners using their phones to disseminate hurtful information about other learners will be dealt with severely and parents will be informed
- No learner should be accessing Facebook or any similar site as these are age restricted sites
- Any videoing or the taking of photographs will not be permitted unless under staff supervision

ANNEXURE A

LEARNER ACKNOWLEDGEMENT FORM

Use of ICTs, including computers, and access to the Internet through the school is a privilege. Users granted this privilege must adhere to strict guidelines concerning appropriate use. All users are required to acknowledge receipt and understanding of guidelines and rules.

I acknowledge that I have received a copy of /the teacher has explained to me the following policies and/or rules:

- 1. Rules for use of Computer Laboratory
- 2. Policy on cell phones for learners
- 3. Policy on acceptable use of the internet and email
- 4. Policy on Cyber Bullying

I understand the contents of these documents and will abide by them. If I am not sure I will ask for further explanation from the person responsible for the laboratory, my class teacher or any other senior teacher in the school.

I also understand that any violation of these policies is unethical and in some cases may constitute a criminal offence. Should I break any of these rules, my access privileges may be withdrawn and disciplinary action and/or appropriate legal action may be taken.

Signed, this	day of	in the year 20
Full name		
ID No —		Date of birth
Class		
Learner's Signature		Witness

ANNEXURE B

PARENT ACKNOWLEDGEMENT FORM

Use of computers and access to the Internet through the school is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. All users are required to acknowledge receipt and understanding of guidelines and rules.

I acknowledge that I have received a copy of the following policies and/or rules:

- 1. Rules for use of Computer laboratory
- 2. Policy on cell phones for learners
- 3. Policy on acceptable use of the internet and email
- 4. Policy on cyber bullying

I agree that I have read and understood these documents and that I will explain them to my child/ren. If I am not sure I will ask for further explanation from the school.

I also understand that any violation of these policies is unethical and in some cases may constitute a criminal offence. Should my child/ren break any of these rules, access privileges may be withdrawn, and disciplinary action and/or appropriate legal action may be taken.

PREAMBLE:

After due consultation between the School Governing Body and Stakeholders, the following policy is introduced.

The purpose of this Policy is to limit the use of cell phones and other electronic devices during official school hours.

The policy must be read in conjunction with the School Code of Conduct and the Demerit Policy of the School and does no aspect of this policy exclude any action sanctioned by such policies, including but not limited to theft, pornography, malicious damage to property and any form of use of any device or electronic media for bullying.

RULES REGARDING CELL PHONES ON THE PREMISES OF THE SCHOOL

- 1. Learners bring cellular phones and other electronic devices to school at own risk and can the School and/or SGB not be held liable for theft or breakage on school property.
- The use of cellular phones and/or any electronic devices during official school hours or during other formal and/or official school functions is prohibited unless authorized to do so by a teacher or other adult.
- 3. Teachers are encouraged to set an example and use cellular phones and other electronic devices sparingly and judiciously.
- 4. A learner who misuses a cell phone on school property to download pornography, offensive or harmful material or sends such material to any other learner(s) while on school property may be found guilty of an offence after a fair hearing for misconduct under the code of Conduct for Learners.

- 5. Any allegation by a learner that another learner is utilizing any electronic device (including but not limited to cellphones and email), to commit any act of bullying (cyber bullying) through the use of pictures or verbally, will be thoroughly investigated. This will be the case whether the incident(s) take place within or outside of school hours, in line with the no-tolerance stance against bullying taken by the GDE.
- 6. A learner who during class, assembly or on any other formal occasion fails to adhere to the Policy may be found guilty of an offence under the Code of Conduct for Learners after a fair hearing.
- 7. Electronic devices found in use as set out above will be confiscated by an educator and handed in at the school office. A learner may collect the item at the end of the school term. A parent may however collect the item at an earlier date.

Signed, this	day of	_ in the year 20
Full name of parent		
Name and surname of learner		
Class of learner		
Parent's Signature ————		

ANNEXURE C

STAFF MEMBER ACKNOWLEDGEMENT FORM

Use of computers and access to the Internet through the school is a privilege. Users granted this privilege must adhere to strict guidelines concerning the appropriate use of this information resource. All users are required to acknowledge receipt and understanding of guidelines and rules.

I acknowledge that I have received a copy of the following policies and/or rules:

1. Rules for use of GoL Computer laboratory

Policy on acceptable	use of the internet and ema	ail
3		
4		
I understand the contents of t	hese documents and will ab	pide by them.
	Should I break any of thes	is unethical and in some cases may se rules, my access privileges may be al action may be taken.
Signed, this	day of	in the year 20
Full name of staff member——	v	
ID number		
Post number		
Designation of staff member—		
Staff member's signature		Witness signature