



SUNLANDS PRIMARY SCHOOL

P O BOX 36037, GLOSDERRY, 7702

PHONE: 021-7978010 FAX: 021-7622697

E-MAIL: cris@sunlands.co.za

WEBSITE: www.sunlands.co.za

IT POLICY

IT ACCEPTABLE USE

Acceptable Use

This section defines the boundaries for the “acceptable use” of the school’s electronic resources, including software, hardware devices and network systems. Hardware devices, software programs and network systems purchased and provided by the school are to be used only for the creating, researching, and processing school-related materials. By using the school’s hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy other applicable school policies, as well as laws and regulations.

Software

All software acquired for or/on behalf of the school or developed by the school or contracted personnel on behalf of the school are and shall be deemed school property. All such software must be used in compliance with applicable licenses, notices, contracts and agreements.

Purchasing

All purchasing of school software shall be centralized with the Principal and Head of IT to ensure that all applications conform to school’s software standards and are purchased at the best possible price. All requests for software must be submitted to the Financial committee for approval.

Licensing

Each educator is individually responsible for reading, understanding and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on school computers. Unless otherwise provided in the applicable license, notice or agreement any duplication of copyrighted software, except for backup and archival purposes, may be a violation of the law on copyright. In addition to violating such laws, unauthorised duplication of software is a violation of the school’s Information Technology Policy.

Software standards

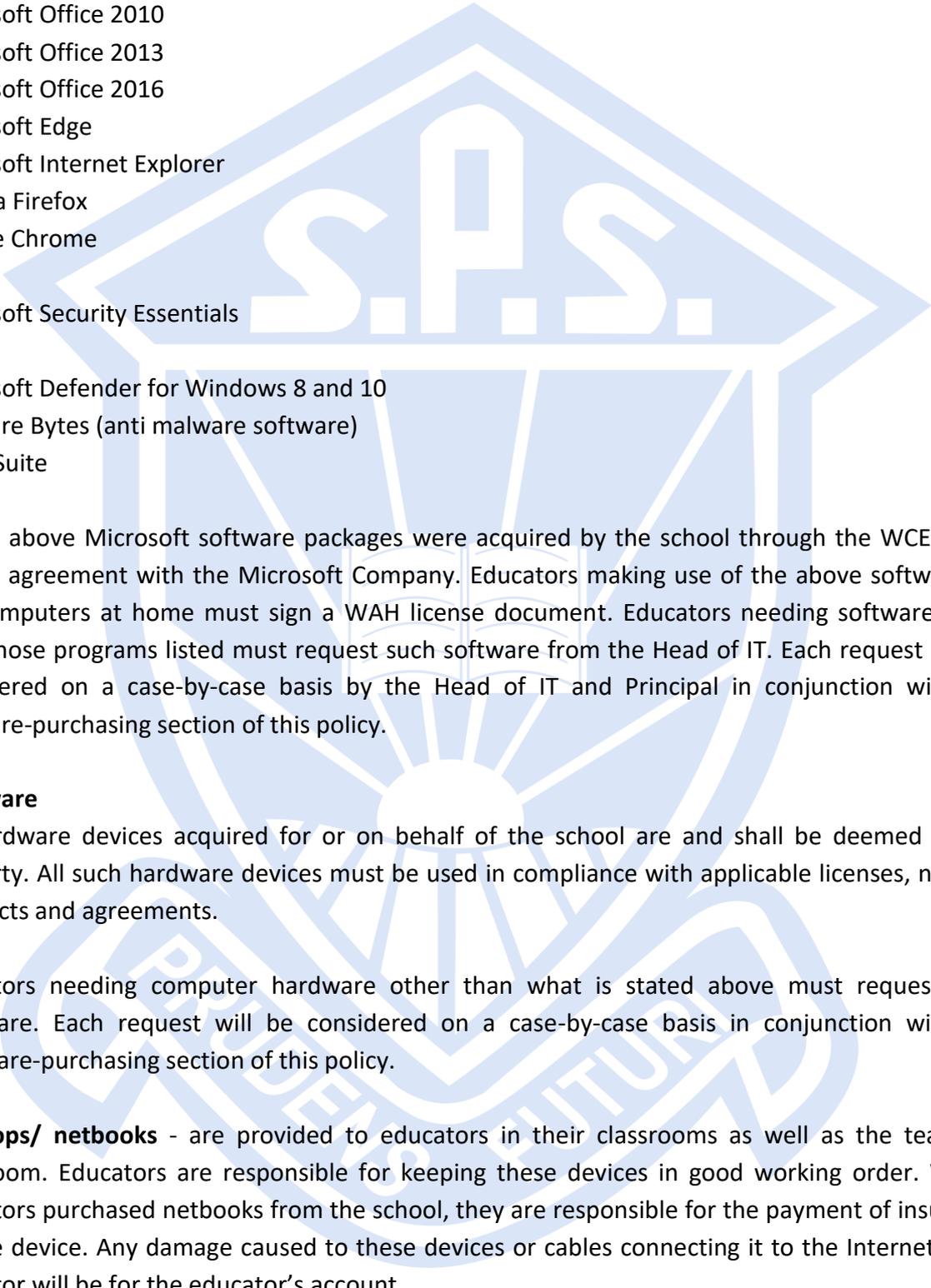
The following list shows the standard suite of software installed on school computers:

Microsoft Windows 7

Microsoft Windows 8.1

Microsoft Windows 10

Microsoft Outlook 2003

A large, light blue watermark logo for S.A.S. (Sarasota Area Schools) is centered on the page. The logo features a shield with a sunburst at the bottom and the letters 'S.A.S.' in a stylized font across the top.

Microsoft Outlook 2010
Microsoft Outlook 2013
Microsoft Outlook 2016
Microsoft Office 2003
Microsoft Office 2010
Microsoft Office 2013
Microsoft Office 2016
Microsoft Edge
Microsoft Internet Explorer
Mozilla Firefox
Google Chrome
Opera
Microsoft Security Essentials
AVG
Microsoft Defender for Windows 8 and 10
Malware Bytes (anti malware software)
CAMI Suite

All the above Microsoft software packages were acquired by the school through the WCED who has an agreement with the Microsoft Company. Educators making use of the above software on the computers at home must sign a WAH license document. Educators needing software other than those programs listed must request such software from the Head of IT. Each request will be considered on a case-by-case basis by the Head of IT and Principal in conjunction with the software-purchasing section of this policy.

Hardware

All hardware devices acquired for or on behalf of the school are and shall be deemed school property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts and agreements.

Educators needing computer hardware other than what is stated above must request such hardware. Each request will be considered on a case-by-case basis in conjunction with the hardware-purchasing section of this policy.

Desktops/ netbooks - are provided to educators in their classrooms as well as the teacher's workroom. Educators are responsible for keeping these devices in good working order. Where educators purchased netbooks from the school, they are responsible for the payment of insurance for the device. Any damage caused to these devices or cables connecting it to the Internet by an educator will be for the educator's account.

Flash drives – will be provided to educators for the purpose of storing school related information, documents and data. These flash drives **may not be used** by an educator's family members or learners in his/her class for personal use as it increases the risk of spreading computer viruses and malware onto the school's IT system. Educators may choose to acquire their own flash drives for school use.

Computer viruses and malware – Educators are responsible to keep their computers in their classrooms and at home virus and malware free to prevent the spread of these viruses and malware and for the protection of our school's IT system and prevention of a possible shut down thereof. All desktops/netbooks should be scanned and that anti-virus software should be updated at least once a week.

The computer laboratory

The computer lab is established for the use of teaching Information Technology to learners. Computers (Information Technology) are offered to all learners from Grade R to Grade 7 at Sunlands Primary School and are integrated with CAPS. The IT Curriculum is fully integrated with the NCS/CAPS and work done in classrooms.

Class and subject educators are not allowed to work in the computer lab **during school hours** as its primary function is being used for teaching learners during that time. Each educator has a computer/netbook for use in his/her classroom for school related work and administrative tasks. Computers with printers are available in the staffroom for school related work and administrative tasks. Computers in the staffroom are not to be used for private purposes as it will prevent other educators from doing school related work on them.

The computer lab will only be available to educators after school with prior arrangement if a computer is available. Should an educator require access to a computer in the lab during any afternoon, a booking or arrangement must be made well ahead of the planned activity (at least 24 hours prior) to give the Computer Educator a chance to change her schedule accordingly. Computers as an extramural activity are offered to our learners to complete school tasks and projects and takes precedence. Computers will be allocated to learners first should an educator request to work in the lab.

IT Policy for learners

Classes are divided towards half a class attending lessons in the computer lab during a session. This enables each learner having access to their own workstation.

When using the computer lab, there are rules that all learners must adhere to:

- Learners are to enter the lab quietly.
- No running, eating or drinking in the IT Centre.
- No computer settings may be tampered with, i.e. changing wallpapers, screensavers and desktop settings.

- Users must log off when they have completed their lessons.
- Keyboards should be placed neatly in front of monitors.
- Chairs must be positioned under tables when learners leave the IT Centre.
- Learners' will not be allowed to change or rename other learners' folder as this action is considered as malicious damage to digital property.
- Storage devices from home will not be connected to computers in the lab to prevent the spread of computer viruses and malware onto our lab's IT system or a possible shut down.

Internet access for learners:

- All learners will have access to Internet resources through the classroom LAN.
- Children are to be supervised at all times when accessing the Internet.
- Learners will not be allowed post personal contact information about themselves or other people on the computers. Personal contact information includes physical home, postal and e-mail addresses, telephone and cell phone numbers, etc.
- When using the internet (www), learners are not allowed to access social media sites, private e-mail or download unauthorized information, programs, music or pictures from restricted sites.
- Learners will not attempt to gain unauthorized access to any other computer system through or go beyond the school's authorized access account. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".
- Learners are not allowed to download programs or files without seeking permission from the Domain Administrator or Computer Teacher first.

Inappropriate language:

- Learners will not use foul, obscene, profane, lewd, vulgar, rude, defamatory, threatening, or disrespectful language.
- Learners will not post information that could cause emotional or psychological damage to a fellow student or educator.
- Learners will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Learners will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
- Learners who make themselves guilty of the mentioned actions will be reported to the SMT who will then take the necessary action.

Where learners deliberately access inappropriate material:

A student will be removed from the computer and all computer privileges are suspended until further investigation. Subsequent offences will lead to heavier penalties, to be decided by the school principal in conjunction with the Heads of Discipline and IT.

IT Policy for Sunlands staff members, Social Media for educators and Best Practices for Guiding Staff in Use of Social Media.

What is social media?

Social media is defined as any form of online publication or presence that allows end users to engage in multi-directional conversations in or around the content on the website. A large percentage of Internet traffic is centered around the use of social media. Social media includes: Facebook, Instagram, Foursquare, Vimeo, Flickr, LinkedIn, My Space, Ning, Twitter, Second Life, YouTube, blogs, Wikis, social bookmarking, document sharing (cloud technologies), SMS's, What's App, other instant messaging applications and email.

What are the purposes of best practices?

Best practices serve to be a guideline regarding the use of social media at Sunlands Primary School. In addition, these guidelines refer to existing school policies, as well as codes of conduct as set out by SACE and the Department of Basic Education, that prohibit certain actions by staff member and learners.

Best Practices

Be Transparent

How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity or misrepresenting your identity. Be honest about who you are, where you work and what you do.

Always a School Employee

The lines between public and private, personal and professional are blurred in the digital world. Even when you have a disclaimer or use a different user name, you will always be considered to be a WCED or SGB employee. Whether it is clearly communicated or not, you will be identified as working for and sometimes representing the school in what you do and say online. Even when using a disclaimer, you still expose yourself to negative consequences that may follow. Always write in the first person and make it clear that you are speaking for yourself and not on behalf of the WCED or Sunlands Primary School.

Use a Disclaimer

Include a disclaimer on your social media site which says something like this: "The opinions and positions expressed on this site are my own and do not necessarily reflect my school or the Education Department's positions, strategies, or opinions." This standard disclaimer does not exempt employees from their responsibilities as explained in these guidelines. If asked by media to comment on a school related issue, refer them to the correct department or person in the circuit or when in doubt, to the principal or Circuit Manager.

School Values

Represent the WCED and the school's values. Express ideas and opinions in a respectful manner. All communications should be done in good taste. Build trust and responsibility in your relationships. Do not denigrate or insult others including learners, staff, administrators, parents, or other districts. Don't use ethnic slurs, innuendos, obscenity or any other inappropriate content. Even though you are of legal age, consider carefully what you post through comments and photos. There are schools who have taken disciplinary action on staff that made posts relative to alcohol and sexual activities. Inappropriate posts lead to the disintegration of responsibility, trust and respect between the school, educators, learners and the community. It takes years to build such relationships, but only one inappropriate incident may cause the breakdown of such relationships between all parties concerned.

Build Community/Positively Represent School

Represent the WCED, school and the learners and parents you serve in the best light. Respect the privacy and the feelings of others. Under no circumstance should offensive comments be made about learners or colleagues (including admin staff) nor the Education Department in general. Negative comments about people may amount to cyber-bullying and could be deemed a disciplinary offence. Your posts and comments should help build and support the school community. Do not comment on nor forward unsupported information, e.g. rumours, political statements, etc. You are responsible for what you post, be certain it is accurate and supports your organization. If you are about to publish something that makes you hesitate, wait a day, review the guidelines and talk to a colleague or supervisor. Once posted you can't take it back. Although what is posted can be deleted, it stays in the cloud on the Social Media Company's servers and can be used against you. Also, even when what is posted can be deleted, it can still be shared and viewed before its removal.

Share your Expertise

Write what you know and be accurate. Add value to the discussion. Post something useful. Provide worthwhile information and perspective. A district's most valuable asset is its staff represented by its people and what you publish may reflect on the school. Speak in the first person with your own voice and perspective.

Respect and Responsibility

Employees, parents, and learners reflect a diverse set of customs, values and points of view. Be respectful for the opinions of others in your posts or comments. You are responsible for the content you post. Consider the words used to tag content in a social bookmarking site. Consider the avatar you select. Do your tags, descriptions, and your image portray you in a professional manner?

Own and Correct Mistakes

If you make a mistake, admit the mistake and correct it quickly. Clearly state when you have corrected a previous post. Even though damage may be done, it is best to admit your mistake and correct it. Apologize where it is appropriate.

Confidential Information

Online postings and conversations are not private. Do not share confidential information whether it is internal school discussions or specific information about learners or other staff. What you post will be seen by others and will be online for a long time. It can be forwarded or shared in just a few clicks. Do not write about colleague or student without their permission. Protect confidential and proprietary info. This refers to personal learner/ staff member information (confidential), what is written in learner workbooks and assessment activities (propriety and confidential).

School Logos

Do not use any school logo or images without permission.

Posting Photos or Movies

Do not post photos of movies without permission. Do not post photos or movies of fellow staff members taken on the school premises. Even an innocent photograph or video can be interpreted wrongly by the community. Do not use photos or movies taken at school without the permission of the Principal. If you feel the need to post them online, it can only be done via the school official social media websites with the assistance of the Head of IT. Do not post photos or movies that contain student without parent consent. Photographs or movies taken of educators off the school premises relating to alcohol or tobacco use may be deemed inappropriate by the parent community. Your postings (comments, photos and movies) on a social media site are an extension of your personality and by that token an extension for your professional life and your classroom. (If it would seem inappropriate to put a certain photograph on a wall at home, is it really correct to put it online?) Parents may report an educator to the WCED if an educator's actions seem inappropriate according to parents' viewpoint, culture and religion. An educator is deemed to be an example to learners, parents and the community and be an upholder of good and acceptable morals and values.

Responding to online Negative Comments and Criticism

How you respond to negative comments or criticism will say more about you and your character than what you post. If you delete a negative post, it discourages open communications. When publicly criticized or receiving a negative comment, first, stay cool and don't reply in haste. Express your view in a clear, logical way. Don't get personal and if you made a mistake, admit it and move ahead. It is not uncommon for a negative response to be answered by some other person, who supports your view. When in doubt, it's best to ignore a comment and not give it credibility by acknowledging it with a response publicly; perhaps a face-to-face meeting would be more appropriate.

Response and Post Regularly

Post regularly. Don't post to your blog and then not post for three weeks. Readers won't have a reason to follow you if they can't expect new content regularly. Respond to other's posts. Answer questions; thank people even if it's just a few words. Make it a two-way conversation.

Spell Check and Abbreviations

Blog and wiki posts should be well written. What you post will be online for the world to read. Follow writing conventions including proper grammar, capitalization, and punctuation. Be cautious about using common abbreviations. While your circle of friends may understand what you are saying, you may have readers from across the world who won't understand. When in doubt, define the abbreviation at least once in a post or include a definitions page on your site.

Social Bookmarking

- Be aware that others can view the sites that you bookmark.
- Be aware of words used to tag or describe the bookmark.
- Be aware of URL (website address) shortening services. It would be best to use the original URL.
- Attempt to link directly to a page or resource if possible as you do not control what appears on landing pages in the future.

Copyright and Fair Use

Respect copyright and fair use guidelines. Share what others have said by linking to the source and using embedded content. Be sure to cite your source when quoting. When using a hyperlink confirm that link goes where it should and that the content is appropriate.

Personal Information

Be careful about sharing too much personal information. People often share information such as their pet name, their parents and children's names, where they grew up, and more. This information has been used by hackers to guess passwords. If you share that you will be out of town, a criminal may use this to target your home for a burglary. Be smart and don't share too much about yourself online.

Video

YouTube is becoming an increasingly popular place to share personally created movies. You are responsible for all you do, say, and post online including video. Anything posted online should represent you in a professional manner as others will see you as connected to the school district. It disrupts learning to have days of conversation about a teacher created YouTube video with questionable content.

Staff-Learner Relations

Employees are prohibited from establishing personal relationships with learners that are unprofessional and thereby inappropriate. Examples of unprofessional relationships include, but are not limited to: employees fraternising or communicating with learners as if employees and learners were peers such as writing personal letters or e-mails; "texting" learners; calling learners on cell phones or allowing learners to make personal calls to them unrelated to homework or class work; sending inappropriate pictures to learners; discussing or revealing to learners personal matters about their private lives or inviting learners to do the same (other than professional counselling by a school counsellor); and engaging in sexualized dialogue, whether in person, by phone, via the Internet, or in writing. Employees who post information on Facebook, My Space or similar web sites that include inappropriate personal information such as, but not limited to: provocative photographs, sexually explicit messages, use of alcohol, drugs or anything learners are prohibited from doing must understand that if learners, parents or other employees obtain access to such information, their case will be investigated by school and WCED and if warranted will be disciplined up to and including termination, depending upon the severity of the offense. Additionally, personnel at the WCED, depending upon the severity of the offense, may have their case forwarded to the DBE for review and possible further sanctions. Due to past incidents, the Sunlands IT team and SMT reserve the right to periodically conduct Internet searches to determine if employees have posted inappropriate materials on-line or were busy with online activities during school hours (07:30-15:00). If inappropriate use of computers and web sites is discovered, the offensive material will be downloaded and promptly brought to the attention of the Principal.

Email

The school requires through acceptable use policies, that all electronic or any other communications by educators to learners/parents at any time, to be professional and acceptable in content. Email between educators, learners and parents shall be done through the school's provided email application. Email must conform to school email policies.

Personal Responsibility

Educators and admin staff are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time. Even when posts are deleted from the visual part of the website, they are still embedded on the social network's database as they are not deleted from the database. In the case of inappropriate made online and deleted afterwards, they can be pulled from the database and be used against the user in a disciplinary hearing or court case. Therefore, protect yours as well as the school's privacy.

Your online behaviour should reflect the same standards of honesty, respect and consideration that you use face-to-face. Remember that all forms of social media are an extension of your classroom. What is inappropriate in you classroom should be deemed as inappropriate online.

The lines between public and private, personal and professional are blurred in the digital and online world. By virtue of identifying yourself on social media online, you are now connected to colleagues, learners, parents, the school community and the world. By posting comments online via social media sites you are broadcasting to the world.

You should ensure that content associated with you is in line with your work policies at Sunlands Primary, SACE and the Education Department. How you present yourself online should be comparable to how you present yourself in person. Comments related to the school should always be of the highest standards of professional discretion. When posting, even with the strictest settings educators should always act on the assumption that all postings are public domain. When contributing online do not post confidential student information. Confidential information may be deemed as events which happened on the school premises, reports by professionals (psychologists, therapists, school counsellors) what is written in learners' workbooks and assessment activities.

An important practice in the cyber world to remember is that a user should not accept friend requests or requested to be linked of people you don't know. By accepting requests or links from unknown persons may compromise your privacy as well as those of family, friends and colleagues you are linked to. You open yourself to abuse, hackers getting hold of password and stealing your identity by using your personal information.

What is posted online in social media has far reaching consequences for your current and future career

Social Media policy for educators

Life revolves around the use of technology and social media. Therefore, the SMT and IT Department understand the need for educators and other staff to collaborate online. Unfortunate and negative events taking place at school and what is done by or written by learners are private and confidential and should stay at school. Posting comments regarding such events is highly unprofessional and inappropriate.

The school and learners should be protected in all educational domains. This includes learners being protected online from all forms of discrimination and ridicule. Comments posted online may lead to instances of bullying and learners being humiliated and may reflect negatively on the school and staff members' reputation.

As staff members and educators we are in a position of trust. Both parents and learners trust us to protect our learners. Comments posted may lead to the breakdown of trust in our relationship with all parties concerned.

Therefore:

1. No comments that may reflect negatively on Sunlands Primary School, its learners, staff members, staffroom chats, meetings and learners' work should it be in workbooks or assessment activities may be posted online on staff members' private social media pages. Future positive comments may be posted online via our school's official Facebook web and blogging pages.
2. No photos taken on the premises, staffroom or where the school is being represented at sports, academic and cultural events may be posted online on staff members' private social media pages. Photographs taken of school events will only be posted on the school's website, official Facebook and blogging pages. This should be done with the assistance of the Head of IT.
3. Being part of the technological age, educators will also regularly make use of Social Media in their private capacity; however, educators will not be allowed to make use of Social Media during school hours (Monday to Tuesday, 07:30-15:00 and Friday, 07:30-12:45) either on their cell phones or other devices such as iPads, tablets, laptops, desktop computers or netbooks in the classrooms, the Teachers' workroom or Library. In the event of a staff meeting, educators will be expected to put cell phones away and refrain from doing any activities such as connecting, checking social media and texting via any social application. Such practices are considered to be unprofessional and disrespectful towards an educator's main purpose to teach. The same is considered for meetings as being unprofessional, disrespectful and rude behaviour towards the person leading the meeting proceedings. No teacher may receive a telephone call or sms in the classroom on during a meeting, unless approved by the leadership for an emergency or as part of a lesson. In the case of a family emergency, the concerned family member may contact the school office. The Admin staff will let the staff member know.
4. Staff members will be held responsible for what is posted on social media.
5. The frequent disregard of the school's IT and social media policy by means of misconduct by staff members will lead to disciplinary hearings involving the SMT and SGB where disciplinary action may be taken against the staff member concerned.
6. The Education Department's IT Policy prohibits teachers and admin staff to link with current parents and learners. Therefore, it is advised that staff members do not link with current parents and learners of our school as it can lead to events that may cause a breakdown of the relationship between the school, educators, parents and learners. Being linked to parents and learners expose educators' private life to all. Any photographs and comments posted can interpreted wrongly and lead to negative career consequences.

Staff Internet Access

All staff will have access to Internet resources via the computer lab, connection points in class, admin offices and the staff workroom. Staff members are requested to use a private email account (Gmail or other applications such as Yahoo, Hotmail, M-Web, etc.) for personal correspondence. The school e-mail accounts (Sunlands Gmail) are to be used for official correspondence so as not to clog the school email systems. Staff members are to respect each-other's privacy with regards to e-mail as they would any other form of correspondence. Staff members are to use their

personal e-mail accounts when signing up for external services that are not bound to the school. Please note the use of an e-mail address as a unique identifier when applying for internet based services often leads to spam, please use your own personal e-mail address for these instances.

Security

Staff members are to seek advice when downloading programs or files from the Head of IT. Educators are to be very careful when connecting learners' flash drives as they often contain computer viruses and malware that may lead to damage of computer hardware, the loss of important documents or totally disabling a computer's hard drive (hard drive crash/ total cleaning out of a hard drive). In the event of connecting learner flash drives, it is of utmost importance that an educator's anti-virus program for protecting the computer should be updated at least once a week to prevent malware from damaging the system and to prevent the spreading of malware through the school's system.

Illegal activities:

Educators will not attempt to gain unauthorized access to any other computer system through or go beyond the school authorized access account. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

Inappropriate language:

Educators will not use foul, obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

Respect for privacy:

Educators will not post information that could cause damage or a danger of disruption. Educators will not engage in personal attacks, including prejudicial or discriminatory attacks. Educators will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.

Access to Inappropriate Material:

Educators will not be allowed to use the school computers to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

Plagiarism and Copyright Infringement:

Teachers need to be aware of copyright laws with regards to information on the World Wide Web. Teachers must enforce these laws with regard to student material taken from the web. The same precautions are to be taken with information from the World Wide Web as those of print. When in doubt, contact the webmaster of the site you seek information from. For any other questions regarding plagiarism or copyright infringement, ask the Head of IT.

School Web Site:

The School's web site is located at <http://www.sunlands.co.za>. The website will be maintained by the website administrator.

Update of the Web Site:

The school website is linked to the school's blogging page on the Internet. Ideally, the website and blogging pages should be updated at least twice per month. Once per month is a recommended minimum. Items to go on the website include children's best work, events and photos of events, prefect reports, cultural information and other items deemed to be newsworthy.

The Domain and Network Administrator (DNA) is responsible for the coordination of the updating of the site. Staff members are encouraged to contribute towards the updating of the blogging pages. Training will be negotiated with the website administration staff.

Policy created: 6 October 2014

Policy updated: 02 February 2017

Policy updated: 29 September 2017

Policy updated: 12 January 2018

Policy updated: 30 July 2019

