Rhenish Girls' High School: Social Media & Social Networking Policy

August 25

2020

This document represents the Rhenish Girls' High School Social Media & Social Networking Policy

Social Media & Social Networking Policy

Table of Contents

1 Introduction

This document is the social media and social networking policy of Rhenish Girls' High School as approved by the school governing body, including its Annexure. This policy seeks to:

1. Regulate the use of social media and social networking at Rhenish Girls' High School
2. Offer learners the opportunities that multimedia learning can provide in a responsible and respectful manner in order to enrich the teaching and learning environment in our school.
3. Outline the responsibilities and behaviour expected of employees, learners and their parents, as users of social media and social networking, in particular, that:
    a. all members of Rhenish Girls' High School community and representatives of the school must take responsibility for the content written, recorded, displayed, posted or communicated online;
    b. they must exercise good judgment and common sense at all times when contemplating any of the listed activities in sub-paragraph (i);
    c. participation on social media and social networking sites may result in the violation of school rules and the learners' Code of Conduct, or be in contravention of existing laws; and
    d. the use or participation in these sites must not negatively affect the name or impact on the reputation of the school.

In general, the school's computer and communication systems are intended for official school purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could have otherwise been used for official purposes; does not interfere with worker productivity; does not detract from any school activity, and does not cause distress, legal problems or morale problems for the school's or other educators, non-educators and learners.

All systems hardware and software are the property of Rhenish Girls' High School. The school has legal ownership of the contents of all files that are stored on its computer and network systems, as well as all messages that are transmitted via these systems. The school reserves the right to access this information without prior notice whenever a genuine business need exists.

The school reserves the right to audit systems on a periodic basis to ensure compliance with this policy.

The school may at its own discretion examine, move or delete files, including electronic mail (e-mail), for purposes of system maintenance or if the files are determined to be disruptive to the system or its users, either intentionally or unintentionally.

The school provides no warranties of any kind, whether expressed or implied, for the services it provides.

The school will not be responsible for any damages suffered while on this system, including loss of personal data due to system outages or irresponsible use.

The school is not responsible for offensive material obtained by any user using the school's information systems.

2 Scope

This policy applies to all employees, learners and their parents at Rhenish Girls' High School. The school respects the individual privacy of educators, non-educators and learners. However, this privacy does not extend to their work-related conduct or to the use of equipment, resources or supplies provided by the school.

The school is committed to the highest standards of conduct and ethics, and its success is built on integrity in all school matters. The school recognises that emerging online collaboration is changing the way in which individuals and organisations communicate, and that social media platforms constitute a large part of people's lives during and after school hours. Therefore, the school encourages ethical and responsible engagement on all social media platforms.

3 Definitions

The following words and terms bear the same meaning assigned to them in the Social Media and Social Networking Policy:

"access" means the right, opportunity or means of funding, or retrieving information;

"child" means a person under the age of 18 years;

"cyberbullying" means wilful and repeated harm inflicted on learners, employees and parents through the use of computers, cell phones and other digital devices, and the associated software and social media platforms;

"social networking site" means a web-based service that allows individuals to:

(a) build a public or semi-public profile;
(b) share contacts or friends with other users; and
(c) view their lists of contacts or friends and those made by others within the system; the nature and nomenclature of these contacts or friends may vary from site to site.

Information systems – the systems consisting of the network of all communication channels used within the school.

Intercept – the aural or other acquisition of the contents of any communication by any means so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient thereof, and includes the —

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any indirect communication; and

(c) diversion of any indirect communication from its intended destination to any other destination.

IT – information technology.

School – the school governing body, as well as any person to whom particular authority or functions have been delegated in terms of this policy.

School management – the principal or a member of the school staff delegated by the principal.

Social media – the means of interaction among people during which they create, share and exchange information and ideas in virtual communities and networks. Social media can include, but is not limited to text, audio, video, images, podcasts, blogs, wikis and photo-sharing, including YouTube, Flickr and Instagram, as well as online social networks such as Facebook, Twitter, LinkedIn, Google+, Myspace and any other multimedia communications.

Social media platforms – blogs, micro-blogs, wikis, social networks, social bookmarking services, user rating services and any other online collaboration, sharing or publishing platform, whether accessed via the web, a mobile device, text messaging or any other existing and/or future communication medium.

Systems hardware – any mechanical or electronic device linked to a computer system, including the central processing unit and added or additional devices such as printers and external disk drives.

Systems software – computer software designed to operate and control the computer hardware and to provide a platform for running application software.

Avatar means: an icon or figure representing a particular person in a computer game, Internet forum, etc.

Blogs means: the blogs or journals where authors and users can post textual, audio and video content, and where some permit others to post comments on their blogs.

Guests means: people using the school's social media space and includes, but is not limited to, visitors, workshop attendees, volunteers, adult education staff and learners, governing body members, Independent contractors, vendors and school consultants.

Media sharing means: using websites where users post and share videos, audio files and/or photos as well as tag them to enable searchability. (Examples include YouTube, Flickr, Picasa and Google Video.)

Microblogs means: websites and spaces that allow users to post short blog entries. (for example, Twitter, Facebook and Foursquare).

Public social media networks means: websites, web logs (blogs), wikis, social networks, online forums, virtual worlds and any other social media generally available to the public or consumers, and which do not fall within the school's electronic technologies network (e.g. MySpace, Facebook, Twitter, LinkedIn, Flickr, YouTube, Edmodo, Yammer.)

School-approved password-protected social media tools means: those tools that fall within the school's electronic technologies network or which the school has approved for educational use.

Social media use means: communication, collaborative sharing, and reaching out to learners, employees and guests for educational purposes, using school-provided websites, platforms, resources or documents. Examples include, but are not limited to, Google Apps, Ning, Teacher Tube, Moodle and Gaggle.

Social networks means: websites where users can create customised profiles and form connections with other users based on shared characteristics and interests.

Users means: learners, employees, guests and others who make use of the school's networks, systems, computers and devices, or any other such devices brought onto the school premises, for carrying out their social media activities.

Virtual world means: web or software-based platforms that allow users to create avatars or representations of themselves, and through these avatars to meet, socialise and contact with other users. (Second life is an example of a virtual world.)

Wikis means: resources or documents edited collaboratively by a community of users with varying levels of editorial control by the website publisher. (Wikipedia is the best known example.)

4 Legal framework

This policy is, among others, underpinned by:

1. Constitution of the Republic of South Africa, 1996
2. United Nations Convention on the Rights of the Child, 1989
3. South African Schools Act, 1996 (Act 84 of 1996)
4. Employment of Educators Act, 1998 (Act 76 of 1998)
5. Western Cape Provincial School Education Act, 1997 (Act 12 of 1997)
6. Western Cape Government Social Media Policy, 2014
7. Electronic Communications Act, 2005 (Act 36 of 2005)
8. Films and Publications Act, 1996 (Act 65 of 1996)
9. Protection from Harassment Act, 2011 (Act 17 of 2011)
10. Criminal Procedure Act, 1977 (Act 51 of 1977)
11. Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007)
12. Copyright Act, 1978 (Act 98 of 1978)
13. Children's Act, 2005 (Act 38 of 2005)
14. Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002)
15. Guidelines on e-Safety in Schools, Department of Basic Education, 2010

In terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, "any person … may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence".[1] The school may therefore intercept any communication that is conveyed through the school's information systems or social media platforms and that refers to any information regarding the school.

5 Internet policy

Internet access shall be granted to employees who have a legitimate need for such access, for which the user needs to formally apply. All internet connections shall be via the approved internet service provider of the school. Any other connections are prohibited.

Internet use is a privilege, which constitutes the acceptance of responsibilities and obligations that are subject to government policies and laws. Acceptable use must be legal, ethical and respectful of intellectual property, ownership of data, systems security mechanisms and individual rights to privacy and freedom from intimidation, harassment and annoyance.

[1] Section 4(1).

Users shall be subject to limitations on their internet use, as determined by the appropriate supervising authority.

To protect the school from profane material and to minimise the use of bandwidth, all internet use shall be monitored by web content filtering software.

Content filtering software shall prevent users from connecting to certain websites that do not relate to school business. All websites that contain sexually explicit, profane and other potentially offensive material shall be blocked via the proxy server.

At any time and without prior notice, school management reserves the right to examine web browser cache files, web browser bookmarks and other information that is stored on or passing through the computers of the school. Such management access ensures compliance with internal policies, assists with internal investigations, and aids in managing the school.

6 E-mail policy

The school does not guarantee privacy or confidentiality of any e-mail.

Use of e-mail to violate this or any school policy is prohibited.

Any use of e-mail that does not reflect the image and reputation of the school is prohibited.

The user bears sole responsibility for all transmissions using his/her assigned e-mail address.

Concealment or misrepresentation of names, addresses or affiliations in e-mail is prohibited.

Use of e-mail for commercial purposes is prohibited.

Use of e-mail that is threatening, offensive or intended for purposes of harassment is prohibited.

E-mail is part of the business or administration record of the school, and may be inspected.

7 Social media and social networking

Social media and social networking are used amongst other reasons to:

1. participate in online communication in order to share an interest and gain or share knowledge;
2. share music, art videos, opinions, collaborate on work or discussions and learn from one another;
3. socialise by keeping in touch with existing friends and finding new ones, and to channel the promotion of a cause or product;

4. allow users to link up with each other quickly and effectively, especially in a professional environment;
5. further professional or personal goals through users communicating their opinions, values and experiences, or by creating impressive online CVs; and
6. assist in lifelong learning and create communities of practice.

8 Aspects for consideration in our school environment

Employees, learners and their parents at Rhenish Girls' High School must give due consideration to the following when using social media and social networking sites:

1. As with all online communication tools, the social media environment has to be managed so that it does not become all consuming.
2. Cognisance must be taken of copyright law when sharing these media and that modifying any work, comment or posting without permission of the author can affect the reputation of the author and other parties. Permission must be obtained at all times.
3. Privacy and circumspection apply as any communication forwarded to others and/or placed in the public domain must give credit to the source.
4. 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 instance when educators and learners, invite or connect on social media, they must be aware that aspects of their profile are visible to other learners and employees.
5. Users must familiarise themselves with privacy settings and avoid sharing information they may not wish to be in the public domain.
6. Users must avoid or take care not to share compromising images or inappropriate messages that may damage their reputation later on in life.

9 Responsibilities with regard to social media and social networking

9.1 The school

The school has drawn up and formally puts in place this policy on the use of social media in order to:

1. sensitise learners and employees to the appropriate etiquette for each online environment; educate learners on critical thinking skills and digital literacy to enable them to navigate safely through the online world;
2. guide learners to understand the need to select the most suitable communication tools for their educational and social experiences;
3. ensure that learners are aware of the potential negative effects of Internet use;
4. teach learners in an age-appropriate manner about the risks and dangers involved in the use of social media, particularly when some of the risks and dangers occur both in the home and school context (i.e. cyberbullying);
5. encourage learners to act responsibly and be aware of the consequences associated with the use of social media;

6. specify when and for what purpose the use of social media platforms are acceptable;
7. ensure that online activities planned by educators only include age-appropriate sites;
8. guide learners to take responsibility and report inappropriate behaviour, or acts that may negatively affect the school and their fellow learners;
9. advise learners and employees of behaviour that may be inconsistent with the Code of Conduct for learners and sanctions that may be imposed if found guilty of misconduct or serious misconduct in terms of the code and of transgressions of applicable legislation in the case of employees;
10. outline a procedure for incidents which may have a potential for criminal accountability;
11. accommodate incidents with child protection dimensions;
12. inform learners and employees about the policy and ensure that the policy is made visible throughout the school; and
13. insert an addendum for signature by each parent, educator and learner – see eSafety Policy.
14. Establish a "Safe School Committee".

9.2 The Safe School Committee

1. A team within the Safe School Committee of Rhenish Girls' High School must manage e-Safety.
2. The team must comprise:
    a. a member of the school management team;
    b. the network administrator;
    c. an IT educator;
    d. an educator – librarian/counsellor/life skills educator;
    e. a representative from the governing body;
    f. a member of the representative council of learners; and
    g. other appropriate specialists, where practicable.
3. The main responsibility of the team is to develop, implement and enforce an acceptable social media policy, underpinned by the Code of Conduct for learners and employees at Rhenish Girls' High School and to ensure that:
    a. all role players at Rhenish Girls' High School are made aware of the content, the policy and consequences likely to flow from non-compliance;
    b. parents are encouraged to take reasonable steps to ensure that learners comply with the policy within and outside school premises; and
    c. all stakeholders are informed of the types of incidents which may potentially attract sanctions and possible criminal accountability.

9.3 Responsibility of a learner

Learners must:

1. keep in mind the global scope of social media and qualify or limit their posts appropriately;
2. be cordial, honest, fair, thorough and transparent when using social media;

3. remember that although the use of social media may be easy, informal, fast and inexpensive, these electronic messages are permanent, transferable records that can affect the reputation of the school;
4. obtain permission for the use of third-party or employee intellectual property rights, including copyright, patents, trademarks and videos;
5. know that it is against the law to:
    a. become involved in identity theft;
    b. participate in hate or cult websites;
    c. buy or sell stolen goods on websites;
    d. divulge personal information or disclose confidential financial information regarding bank and credit cards by using unsecured bogus sites; and
    e. publish compromising information which may harm another individual's reputation or dignity; it is also regarded as harassment to do something that they know could cause harm to another person, whether mental, psychological, or physical harm.

9.4 Responsibility of the employee

1. The employee must not have online communication on a one-on-one basis with a learner except for formal educational subject purposes, and otherwise always in a group context, for education purposes and for information sharing.
2. The employee must never invite or follow learners on social media, except on those sites which have been designed specifically for professional purposes in a group setting.

9.5 Responsibility of the educator

The educator must:

1. guide learners to understand that what is permissible in a classroom, is acceptable online; and anything that is impermissible in a classroom, is also unacceptable online;
2. be aware that online activities may impact on their personal reputation, image and ability to interact with colleagues and learners;
3. be professional and courteous when interacting with others online;
4. respect the needs for discretion and confidentiality with regard to personal information, and other sensitive information that may not be appropriate for public discussion;
5. endeavour, within the bounds of reason, to remain neutral, objective and professional on issues presented and discussed by educational platforms or sites intended for educational purposes; and
6. judiciously remove any material deemed offensive, inappropriate, off-topic, discourteous or otherwise annoying to other users, upon identifying or being made aware of such material.

10 Policy on Social Media for Employees

10.1 Policy purpose

Social media and general internet use is a valuable part of our society, and it is up to each individual in the school community to make best use of social media to promote the school's excellence. The purpose of the Rhenish Girls' High School Social Media Policy for Employees is to establish rules and provide guidance for employees and guests (collectively known as "users") on the use of social media; to establish a culture of transparency, trust and integrity in social media activities; and to encourage the integration of social media into our teaching and learning environments.

1. Rhenish Girls' High School School recognises the value of teaching enquiry, investigation and innovation using new technology tools to enhance the learning experience.
2. The school also recognises and accepts its authority and responsibility to protect minors from inappropriate content; and its obligation to teach responsible and safe use of the new technologies, as well as the importance of online social media networks as communication and e-learning tool.
3. In line with these values and responsibilities, the school will exercise its right to limit public access to various aspects of the social media within its own social media environment
4. With a view to implementing the school's aims and responsibilities, and responding to new technologies, this policy addresses employees' use of publicly available social media networks, including the following: personal websites, web logs (blogs), wikis, social networks, online forums, virtual worlds and any other social media.

10.2 Social network provisioning and usage

1. In striving to meet its aims and obligations in terms of media and technology involvement, the school provides password-protected social media tools and school-approved technologies for e-learning and encourages the use of school tools for collaboration by employees.
2. The above notwithstanding, public social media networks outside of those approved by the school may not be used for classroom instruction or school-sponsored activities without the prior authorisation of principal or his/her delegate, and parental consent for learner participation on social networks.

10.3 The school's rights and authority

1. The principal and or his/her delegate are granted authority through this policy to create rules, administrative and other regulations and protocols for the carrying out of the purpose of this policy.
2. Within the social media context, users are required to comply fully with this policy and its accompanying administrative regulations and all other relevant school policies, regulations, rules, procedures, social media terms of use and other legal documents, as well as local, provincial and national laws concerning social media.

3. All cyber actions by users attached to the school in any way must be conducted in accordance with the law, assist in the protection of the school's resources, ensure compliance with this policy and its administrative regulations, as well as other school policies, regulations, rules and procedures, social media and Internet service providers' terms, and local, provincial and national laws.
4. The school has a right, but not a duty, to inspect, review or retain any electronic communication created, sent, displayed, received or stored on or over the school's electronics systems; and to monitor, record, check, track, log, access or otherwise inspect the content of its systems.
5. In addition, and in accord with the law, the school has the right, but not a duty, to inspect, review or retain any electronic communications created, sent, displayed, received or stored on users' personal computers, electronic devices, networks, internet or electronic communication systems; and also in data-bases, files, software, and media that contain school information and data.
6. Also, in accordance with the law, the school has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received or stored on another entity's computer or electronic device when users bring to and use such other entities' computers or electronic devices at a school location, function or event, or connect it to the school network and/or systems, or any system that contains school programs, or school data or information.
7. The school will cooperate to the extent legally required of it with social media sites, internet service providers, local, provincial and state officials in investigations or with other legal requests, whether the actions be criminal or civil.
8. If any user believes that there is a conflict in the requirements with which he or she is obligated to comply, the matter must be brought to the attention of a supervisor, principal or media administrator who will follow through with the matter.

10.4 School expectations of its employees

1. Senior executives and workplace/line managers are required to ensure that this policy is understood by staff members working within their area of control.
2. As the line between professional and personal relationships is blurred within the social media context, the school takes no position on an employee's decision to participate in the use of social media networks for personal use during personal time: however, use of these media for personal use during school time is prohibited.
3. It is the responsibility of all users to consider carefully their behaviour and what they place online when communicating with, or "friending" any individual.
4. When employees choose to engage with, or join the school's learners, families or fellow employees in a social media context that exists outside of those approved by the school, they are expected to maintain their professionalism as school employees and to accept responsibility for addressing or reporting inappropriate behaviour or activity by learners of the school or their own school colleagues on these networks.
5. Staff members should not engage in social interaction with learners through social networking sites unless there is an educationally valid context. In the event of a

complaint or allegation being received by the school in this regard, the responsibility will be on the staff member to demonstrate that the use was appropriate.

6. Users should have no expectation of privacy in anything they create, store, send, receive or display on or over the school's various electronic systems, or the school's authorised third-party systems, including their personal files or any of the use of these systems.
7. All employees are expected to serve as positive ambassadors for the school and to remember that they are role models for the learners in this community, and must be respectful and professional in all communications (whether by word, image or other means).
8. Staff may not coerce others into providing passwords, login details or other security access information to them so that they may access social media or locations that they have no authorisation to access.
9. The school reserves the right to access, view, record, check, receive, monitor, track, log, store or otherwise inspect and utilise any or all of its own systems, as well as authorised third-party systems, and to monitor and allocate file server space.
10. Users using the school's systems or authorized third-party systems used on or via the school premises or networks to transmit or receive communications and information shall be deemed to have consented to having the content of any such communication accessed, viewed, recorded, checked, received, monitored, tracked, logged, stored or otherwise inspected or utilised by the school, and to monitor and allocate file server space.
11. Passwords and message delete functions do not restrict the school's ability or rights to access such communications or information.
12. Anything posted on an employee's website or web blog, or any Internet content for which the employee is responsible, will be subject to all school policies, rules, regulations and guidelines.
13. The school is entitled to view and monitor an employee's website or web blog at any time without consent or previous approval.
14. Where applicable, employees may be asked to disclose to the school the existence of and to provide access to, such employee's website or web blog or other personal social media network as part of an employment selection, promotion or disciplinary process.

10.5 Inappropriate usage

1. Employees shall not use obscene, profane or vulgar language on any social media network, nor engage in communication or conduct that is racist, harassing, threatening, bullying, libellous or defamatory; or that discusses or encourages any illegal activity or the inappropriate use of alcohol or illegal drugs; improper sexual behaviour, sexual harassment or bullying.
2. Employees may not use their school e-mail addresses for communications on public social media networks that have not been approved by the school.
3. Employees must make it clear that any views expressed are their own, and do not necessarily reflect the views of the school.

4. Employees may not act as a spokesperson for the school, or post comments as a representative of the school, except when authorised to do so by the principal or the principal's delegate.
5. Employees may not disclose information on any social media network that is confidential or proprietary to the school, its learners or employees, or that is protected by data privacy laws.
6. Employees may not use or post the school's logo on any social media network without permission from the principal or his/her delegate.
7. Employees may not post images of co-workers on any social media network, without the permission of such co-worker.
8. Employees may not post images of learners on any social media network without written parental consent, except for images taken in the public arena, such as at sporting events or public performances.
9. Employees may not post any non-public images of the school premises and property, including floor plans.
10. Because other users of social media networks may view the employee as a representative of the school, the school requires/expects employees to observe the following rules when referring to the school, its learners, programmes, activities, employees, volunteers or communities on any social media networks:
    a. An employee's use of any social media network and an employee's postings, displays or communications on any social media network must comply with all regulations and laws, and any applicable school or departmental policies.
    b. Employees are responsible for their own behaviour when communicating on social media, including being held accountable for the content of the communications that they post, state or on-send on social media locations.
    c. Employees should note that information that they place in the social media, even though it may be designated as private, can be accessed for litigation purposes, distributed by friends and can be accessed in various other legal ways.
    d. Inappropriate communications may not be posted on social media, including but not limited to:
        i. confidential, personally identifiable or sensitive school information about learners, employees and guests;
        ii. child pornography, sexually exploitative material, bullying/cyber bullying or inappropriate commercialisation of childhood experiences;
        iii. defamatory or discriminatory statements or images;
        iv. infringed-upon intellectual property, such as copyright ownership;
        v. terroristic threats; and
        vi. illegal items or activities.

10.6 Interaction with social media groups

1. The school recognises that learner groups or members of the public may create social media platforms representing learners or groups within the school.

2. When employees, including coaches and consultants, choose to join in or engage with these social networking groups, they do so as an employee of the school.
3. Employees have a responsibility for maintaining appropriate employee-learner relationships at all times, and also for addressing or reporting inappropriate behaviour or activity on social media networks. This includes acting to protect the safety of minors online.
4. Employees who participate in social media networks may include information about their work at school as part of their personal profile, as it would relate to a typical social conversation. This may include:
    a. Work information included in a personal profile, but such information must include the job title and job duties.
    b. Status updates regarding the employee's own job promotion.
    c. Personal participation in school-sponsored events, including volunteer activities.

10.7 Consequences of any breach of this policy

1. This policy and its various rules, regulations or guidelines, incorporate all other relevant school policies, such as, but not limited to, learner and employee discipline policies, codes of conduct, acceptable use policies, copyright and anti-discrimination policies.
2. General rules for behaviour, ethics and communications apply when using social networking systems and information, in addition to the stipulations of this policy and the school's various regulations.
3. Users must be aware that violations of this policy or other rules or guidelines on social media may result in loss of access and a variety of other disciplinary actions, including, but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspension, dismissal, breach of contract penalties provided for in statutes, regulations or other laws, as well as legal proceedings on a case-by-case basis.

11 Policy on Social Media for learners

11.1 Policy purpose

Social media and general internet use is a valuable part of our society, and it is up to each individual in the school community to make best use of social media to promote the school's excellence. The purpose of the Rhenish Girls' High School Social Media Policy for Learners is to establish rules and provide guidance for learners on the use of social media; to establish a culture of transparency, trust and integrity in social media activities; and to encourage the integration of social media into our teaching and learning environments.

1. Rhenish Girls' High School recognises the value of teaching enquiry, investigation and innovation using new technology tools to enhance the learning experience.

2. The school also recognises and accepts its authority and responsibility to protect minors from inappropriate content; and its obligation to teach responsible and safe use of the new technologies, as well as the importance of online social media networks as communication and e-learning tool.

3. In line with these values and responsibilities, the school will exercise its right to limit public access to various aspects of the social media within its own social media environment

4. With a view to implementing the school's aims and responsibilities, and responding to new technologies, this policy addresses learners' use of publicly available social media networks, including the following: personal websites, web logs (blogs), wikis, social networks, online forums, virtual worlds and any other social media.

11.2 Social network provisioning and usage

1. In striving to meet its aims and obligations in terms of media and technology involvement, the school provides password-protected social media tools and school-approved technologies for e-learning and encourages the use of school tools for collaboration by employees.

2. The above notwithstanding, public social media networks outside of those approved by the school may not be used for classroom instruction or school-sponsored activities without the prior authorisation of principal or his/her delegate, and parental consent for learner participation on social networks.

11.3 The school's rights and authority

1. The principal and or his/her delegate are granted authority through this policy to create rules, administrative and other regulations and protocols for the carrying out of the purpose of this policy.

2. Within the social media context, users are required to comply fully with this policy and its accompanying administrative regulations and all other relevant school policies, regulations, rules, procedures, social media terms of use and other legal documents, as well as local, provincial and national laws concerning social media.

3. All cyber actions by users attached to the school in any way must be conducted in accordance with the law, assist in the protection of the school's resources, ensure compliance with this

policy and its administrative regulations, as well as other school policies, regulations, rules and procedures, social media and Internet service providers' terms, and local, provincial and national laws.

4. The school has a right, but not a duty, to inspect, review or retain any electronic communication created, sent, displayed, received or stored on or over the school's electronics systems; and to monitor, record, check, track, log, access or otherwise inspect the content of its systems.

5. In addition, and in accord with the law, the school has the right, but not a duty, to inspect, review or retain any electronic communications created, sent, displayed, received or stored on users' personal computers, electronic devices, networks, internet or electronic communication systems; and also in data-bases, files, software, and media that contain school information and data.

6. Also, in accordance with the law, the school has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received or stored on another entity's computer or electronic device when users bring to and use such other entities' computers or electronic devices at a school location, function or event, or connect it to the school network and/or systems, or any system that contains school programs, or school data or information.

7. The school will cooperate to the extent legally required of it with social media sites, internet service providers, local, provincial and state officials in investigations or with other legal requests, whether the actions be criminal or civil.

8. If any user believes that there is a conflict in the requirements with which he or she is obligated to comply, the matter must be brought to the attention of a supervisor, principal or media administrator who will follow through with the matter.

11.4 School expectations of its learners

1. Responsible staff members are required to ensure that this policy is understood by learners working within their area of control.

2. As the line between professional and personal relationships is blurred within the social media context, the school takes no position on an individual learner's decision to participate in the

use of social media networks for personal use during personal time: however, use of these media for personal use during school time is prohibited.

3. It is the responsibility of all users to consider carefully their behaviour and what they place online when communicating with, or "friending" any individual.

4. Learners and parents must understand that when employees choose to engage with, or join the school's learners, families or fellow employees in a social media context that exists outside of those approved by the school, the employees are expected to maintain their professionalism as school employees and to accept responsibility for addressing or reporting inappropriate behaviour or activity by learners on these networks.

5. In similar vein, learners and parents need to recognise that staff members have been told that they should not engage in social interaction with learners through social networking sites unless there is an educationally valid context. In the event of a complaint or allegation being received by the school in this regard, the school will follow through and investigate the matter, and responsibility will be on the staff member to demonstrate that the use was appropriate.

6. Users should have no expectation of privacy in anything they create, store, send, receive or display on or over the school's various electronic systems, or the school's authorised third-party systems, including their personal files or any of the use of these systems.

7. All learners are expected to serve as positive ambassadors for the school and to be respectful in all communications (whether by word, image or other means).

8. Learners may not coerce others into providing passwords, login details or other security access information to them so that they may access social media or locations that they have no authorisation to access.

9. The school reserves the right to access, view, record, check, receive, monitor, track, log, store or otherwise inspect and utilise any or all of its own systems, as well as authorised third-party systems, and to monitor and allocate file server space.

10. Users using the school's systems or authorized third-party systems in use on or via the school premises or network to transmit or receive communications and information shall be deemed to have consented to having the content of any such communication accessed, viewed, recorded, checked, received, monitored, tracked, logged, stored or otherwise inspected or utilised by the school, and to monitor and allocate file server space.

11. Passwords and message delete functions do not restrict the school's ability or rights to access such communications or information.

12. Anything posted on a learner's website or web blog, or any Internet content for which the learner is responsible, is subject to all school rules, regulations and guidelines.

13. The school is entitled to view and monitor a learner's website or web blog at any time without consent or previous approval.

11.5 Inappropriate usage

1. Learners shall not use obscene, profane or vulgar language on any social media network, nor engage in communication or conduct that is racist, harassing, threatening, bullying, libellous or defamatory; or that discusses or encourages any illegal activity or the inappropriate use of alcohol or illegal drugs; improper sexual behaviour, sexual harassment or bullying.

2. Learners may not use their school e-mail addresses for communications on public social media networks that have not been approved by the school.

3. Learners must make it clear that any views expressed are their own, and do not necessarily reflect the views of the school.

4. Learners may not act as a spokesperson for the school, or post comments as a representative of the school, except when authorised to do so by the principal or the principal's delegate.

5. Learners may not disclose information on any social media network that is confidential or proprietary to the school, its learners or employees, or that is protected by data privacy laws.

6. Learners may not use or post the school's logo on any social media network without permission from the principal or his/her delegate.

7. Learners may not post images of other learners on any social media network without written consent from the parent of the learner whose image is to be posted, and also from the principal (or his or her delegate), except in the case of images taken in the public arena, such as at sporting events or public performances.

8. Learners may not post any non-public images of the school premises and property, including floor plans.

9. Because other users of social media networks may view the learner as a representative of the school, the school requires/expects learners to observe the following rules when referring to the school, its learners, programmes, activities, employees, volunteers or communities on any social media networks:

    a. A learner's use of any social media network and a learner's postings, displays or communications on any social media network must comply with all regulations and laws, and any applicable school or departmental policies.

    b. Learners are responsible for their own behaviour when communicating on social media, including being held accountable for the content of the communications that they post, state or on-send on social media locations.

    c. Learners should note that information that they place in the social media, even though it may be designated as private, can be accessed for litigation purposes, distributed by friends and can be accessed in various other legal ways.

    d. Inappropriate communications may not be posted on social media, including but not limited to:

        I. confidential, personally identifiable or sensitive school information about learners, employees and guests;

        II. child pornography, sexually exploitative material, bullying/cyber bullying or inappropriate commercialisation of childhood experiences;

        III. defamatory or discriminatory statements or images;

        IV. infringed-upon intellectual property, such as copyright ownership;

        V. terroristic threats; and

        VI. illegal items or activities.

11.6 Interaction with social media groups

1. The school recognises that learner groups or members of the public may create social media platforms representing learners or groups within the school.

2. When employees, including coaches and consultants, choose to join in or engage with these social networking groups, they do so as an employee of the school, and their status and standing vis-a-vis their learners is not altered by the fact that engagements take place on social networks.

3. Learners have a co-responsibility for maintaining appropriate teacher-learner and learner-learner relationships at all times, and also for reporting or addressing inappropriate behaviour or activity on social media networks. This includes acting to protect the safety of minors online.

11.7 Consequences of any breach of this policy

1. This policy and its various rules, regulations or guidelines, incorporate all other relevant school policies, such as, but not limited to, learner discipline policies, codes of conduct, acceptable use policies, copyright and anti-discrimination policies.

2. General rules for behaviour, ethics and communications apply when using social networking systems and information, in addition to the stipulations of this policy and the school's various regulations.

3. Users must be aware that violations of this policy or other rules or guidelines on social media may result in loss of access and a variety of other disciplinary actions, including, but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspension and/or expulsion, as well as legal proceedings on a case-by-case basis.

12 Prohibited activities or behaviour

The following activities and/or behaviour are prohibited:

1. Copying material bearing copyrights or patents, without proper licensing or authority

2. Using the school's information systems for political lobbying, personal gain or commercial purposes

3. Copying or removing software from the school's computers

4. Downloading material from the internet that is not related to official school activities or business

5. Installation of system hardware or software by unauthorised personnel. Under no circumstances shall unlicensed software, privately owned software, games, public-domain software, and freeware, shareware or demonstration software be loaded onto official computer equipment without prior written consent from the governing body.

6. Using the school's information system for offensive or harassing material. The following shall constitute computer harassment: (1) using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures or other materials, or threats of bodily or psychological harm to the recipient; (2) using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) using the computer to contact another person repeatedly regarding a matter about which one does not have the legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) using the computer to disrupt or damage the academic research, administrative or related pursuits of the school or another person; (5) using the computer to invade the privacy, academic or otherwise, of another, or the threatened invasion of privacy of another; and (6) material containing sexist, racist and/or violent content.

7. Using the school's information system for discriminatory material. Users must have respect for all persons, and avoid discriminatory behaviour towards and victimisation of other social media users, whether on the basis of gender, race, class, creed, colour, sexual orientation, marital or family status, age, nationality, political belief, religion or disability.

8. Viewing or transmission of any material that violates any national, provincial or international law

9. Use of school information systems to gain unauthorised access to any system or data

10. Accessing, downloading, storing or transmitting obscene material through the school's computer network system

Each educator and non-educator shall be granted access to information as needed to perform his or her assigned function, but shall not be given access to information otherwise requiring protection unless and until such access is needed and formally authorised. Authorised users are responsible for the security of their passwords and accounts.

The following acts of 'cyber-misconduct' are prohibited:

1. 'Cyber-loafing' and the abuse of the employer's resources: Educators, non-educators and learners are prohibited from using the school's resources, e.g. computers, telephones, etc., for private purposes during or outside school time, thereby abusing the employment relationship.

2. Creating disharmony and distributing offensive or abusive material: Educators, non-educators and learners may not circulate information that is racist, defamatory, sexist or pornographic. This constitutes gross misconduct. Racist comments are not only offensive, but create disharmony among people.

3. Derogatory statements: Educators, non-educators and learners may not post or distribute derogatory and offensive messages about the school, its staff or the learners. An offender may be found guilty of bringing the school into disrepute, which could lead to disciplinary action or legal action for defamation.

4. Breach of trust: Educators, non-educators and learners may not use the school's information, information systems or social media platforms in a way that breaches the school's trust.

13 Engaging in social media communication on behalf of the school

1. Only persons who are authorised by the school governing body ("authorised persons") may engage in social media communication on behalf of the school.
2. Only authorised persons may comment on any aspect of the school and/or any matter in which the school is involved. When making such comment, the authorised person must identify him/herself.
3. An authorised person who engages in social media communication on behalf of the school must ensure that he/she is familiar with the school's view on specific issues, and should not express views that are inconsistent with those set out by the school.
4. If an authorised person is not familiar with or is unsure of the school's position on any particular issue, he/she should seek clarity from the school governing body.
5. The school may instruct authorised persons to avoid certain subjects/topics, and has the right to monitor and review authorised persons' comments and submissions. The school shall take appropriate action against any authorised person who makes comments or submissions that have not been authorised by the school.

Educators, non-educators, learners and parents using social media for official and non-official purposes should be aware of the following:

The approved social media sites may only be used for official purposes when using the school's information systems.The message that the school wants to convey to other users must be clearly defined.

Postings must be kept legal, ethical and respectful.

Educators, non-educators and learners may not engage in online communication activities that could bring the school into disrepute, and have a responsibility to avoid establishing online relationships and/or interests that could adversely influence or impair their capacity to act with integrity and objectivity in relation to the school as well as other educators, non-educators and learners. In addition, they should refrain from engaging in any social media activities that may bring the school into disrepute, and will be held accountable for any such behaviour.

Personal details of educators, non-educators, learners and parents may not be disclosed. Educators, non-educators, learners and parents should take note that the school may from time to time share photos on social media sites that were taken during official school activities. People may then be 'tagged'. Users of these social media sites are advised to check their security settings if they prefer to review postings in which they were 'tagged'. Educators, non-educators and learners are advised to block other users who they do not know or do not want to be associated with, from accessing their profiles.

The school does not accept any responsibility or liability for weak security settings on the social media profile of any person associated with the school.

If any educator, non-educator, learner or parent posts a remark, photo or video on any social media platform that may harm the reputation of the school, and affiliation to the school is identified, known or presumed, such educator, non-educator or learner will be subject to disciplinary and legal action. Legal action may be taken against a parent who jeopardises the school's reputation.

All information that is published must be accurate, and confidential information may not be disclosed.

Copyright laws must be adhered to.

Only the official approved logo of the school may be used when participating in social media communication on behalf of the school.

Statements to the media must first be approved by the governing body.

All school information systems privileges shall be promptly terminated when an educator or non-educator ceases to provide services to the school, or when a learner leaves the school. The school reserves the right to revoke any user's privileges at any time.

Conduct that interferes with the normal and proper operation of information systems, adversely affects the ability of others to use these information systems, or is harmful or offensive to others shall not be permitted.

14 Server security

1. Where feasible, all servers hosting data and applications shall be located in a physically secure environment where access is strictly controlled. All server rooms shall be regarded as high-risk security areas, to which access shall be strictly controlled.
2. All servers shall be loaded and protected with the latest, approved anti-virus software. Updates for patches and upgrades shall be implemented regularly by the designated IT service provider or the school's IT specialist, when required.
3. Only an authorised administrator shall be granted administrative rights to the servers. Administrative passwords shall be kept secret, and only personnel who have been nominated at the school's discretion shall have access to the passwords.
4. All business or administrative critical data on local computer and notebook hard drives must be copied or moved to a "My Documents" share on a file server, where it will be backed up. Where such an action is not possible, for example due to being away from access to the school network, the data must be copied over on the first available opportunity. It will be the sole responsibility of the user to backup and maintain data security at all times.

   Servers shall be backed up on a monthly basis by the IT service provider or the school's IT specialist.

15 Acceptance of personal responsibility

Any person who uses an information system of the school shall be responsible and accountable to follow recommended procedures, and to take all reasonable steps to safeguard the information handled by that system as well as any sensitive assets involved. The user is solely responsible for all materials viewed, stored or transmitted from school-based computers. However, the school expects users to comply with all school rules. Failure to do so may result in the suspension or revocation of a user's access privileges as well as disciplinary measures, including the possibility of civil and/or criminal liability. Educators and non-educators who fail to adhere to this policy will be subject to disciplinary proceedings in terms of either the grievance and disciplinary procedure of the school or procedures conducted by the Department of Basic Education. Learners who fail to comply with this policy will be subject to the school's code of conduct for learners.

16 Non-compliance

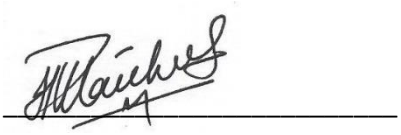
Non-compliance by learners and employees must be dealt with through the school's Code of Conduct for learners, the Employment of Educators Act, 1998 (Act 76 of 1998) and the Public Service Act, 1994 (Proclamation 103 of 1994).

17 Implementation of the policy

The school governing body may from time to time amend, supplement, modify or alter this policy.

This policy is signed into being:

SIGNED AT ___Stellenbosch_____ ON THIS _____30_____ DAY OF___November_ 2020.



Governing body chair

School principal

Acknowledgements: in drawing up this policy RGHS has the drawn on the following sources:

- FEDSAS
- Don't film yourself having sex: Sadleir and De Beer
- Cyber law: maximising safety and minimising risk in classrooms: Bissonette
- Kodak online; Intel.com; IBM.com
- South Africa's Government Communication and Information System; and various school, education district and state social media policies in the USA and Australia

Annexure 1: Safety risks relating to the use of social media and social networking

1. Introduction

The rapid development of electronic access, social networking sites and widespread access to mobile telephony has provided powerful avenues for sharing digital information and content in South Africa. However, these digital mediums have also created an online arena for risks. While there are countless benefits to the use of social technology, including:

(a) rewarding social connections;
(b) creating opportunities for academic and social support; and
(c) identity exploration and cross-cultural interactions,

social media has the potential to expose learners to high-risk content and individuals they may not otherwise have had contact with.

2. Risks associated with social media and social networking

The often uncensored and unmonitored nature of the cyber environment can expose learners to a number of dangers, some of which are briefly defined below.

2.1 Cyberbullying

1. The traditional notion of face-to-face bullying has expanded into the digital realm where offline bullying is extended to acquaintances and strangers online.
2. Even though bullying is a phenomenon that existed well before the creation of mobile phones and the Internet, the two mediums have magnified the problem by creating a new avenue through which bullying can take place.
3. When perpetrated *via* telephone mediums or online, cyberbullying is eased by the apparent anonymity and distance from the victim.
4. This has become a safety risk in South Africa among boys and girls who are victims of online stalking, harassment and cyberbullying, with resulting emotional stress; mostly perpetrated by voice calls, text messages and instant messaging.

2.2 Violence

The term "violence" must be interpreted to include the impact of, and the need to address non-physical and/or non-intentional forms of harm such as, among others, neglect and psychological maltreatment and in particular, mental violence. This includes psychological bullying and hazing by adults or other children; including *via* information and communication technologies such as cell phones and the Internet (also known as cyberbullying).

2.3 Sexting

1. Sexting is the act of sending nude or semi-naked photos or videos, and sexually suggestive messages by mobile phone texting or instant messaging.
2. It is considered a punishable crime under South African law as a form of communication to children under the age of 16 years.

2.4 Sexually explicit and child abuse images and videos

1. Access to and the use of social media presents opportunities for children to be exposed to disturbing, harmful and age-inappropriate content online.
2. However, there have been recent attempts by government to protect children from harmful online content through cell phone pornography legislation which makes it illegal for Internet and cell phone service providers to distribute pornography, or permit it to be distributed, so as to ensure protection for children and women.

2.5 Talking to and meeting with strangers

1. The digital world presents an opportunity for individuals to exchange ideas and content without meeting in person.
2. Information sharing and chatting online can often prompt individuals to meet in person.
3. This practice has had incredible repercussions for children who choose to meet with online friends face-to-face.
4. This allows for certain online risks to emerge, such as learners who may be granted access to digital platforms by falsifying their age online, and adults who may falsify their information and age to pose as teenagers and in doing so establish harmful online relationships with unsuspecting children.

2.6 Plagiarism and personal responsibility

1. Young people who download and swap music files, "cut and paste" homework assignments from other individuals' work, or purchase whole assignments from online "cheating sites", ignore copyright law that applies to the Internet and contribute to crimes such as the pirating of music, images, videos or software in an illegal and dishonest manner.
2. Documented permission is required for the use of third-party or intellectual property rights belonging to another person, including copyright, patents, trademarks, photos or videos, and other intangible property.
3. It is essential that a user obtains permission before photos or videos of other users are posted on the Internet.