EBENEZER

1860

Rhenish Girls' High School: ICT & eSafety Policy

August 25

2020

This document represents the Rhenish Girls' High School ICT & eSafety Policy

ICT & eSafety Policy

Table of Contents

ICT AND E-SAFETY POLICY

1 Introduction

This document is the information systems and e-safety policy of Rhenish Girls' High School as approved by the school governing body. The policy has been drafted in accordance with the provisions of the Constitution of South Africa, 1996; the South African Schools Act 84 of 1996 ('SASA'); the National Education Policy Act 27 of 1996; applicable provincial legislation on school education, and the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

The purpose of this policy is to govern the use of the school's information systems in conveying any communication-related information, and the appropriate use of social media platforms by educators, non-educators and learners. The school recognises the evolution of social media as a mode of communication, but also realises that to optimise the use of social media, it must be used responsibly.

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.

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". 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.

2 Philosophy

The school is committed to the highest standards of conduct and ethics, and its success is built on integrity in all school matters.

1. Given that information is a valuable asset that is critical to the efficient operation of the school, it is recognized that the value of the School's information as an institutional resource and asset is increased by its integrity and appropriate use.
2. Conversely, its institutional value is diminished by insufficient capture, retention and destruction practices; compromised protections; or unnecessary restrictions on its access.
3. It is therefore essential that governance control over information and information systems be in place. This is recognised as an important aspect of the role of the school governing body

(SGB), and IT in all its forms and iterations needs to be governed in terms of laid-down structures and policies.

3 Scope

This policy applies to all users of the school's information and information systems. It also applies to the expression of opinions and comments by educators, non-educators and learners on social media that may in any manner be linked to the school.

4 Definitions

The following words and terms bear the same meaning assigned to them in the ICT & eSafety 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 meida 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.)

5 General

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 need exists, at the discretion of the school.

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.

6 Responsibilities

1. in the light of the above, this policy lays down that the governance of the IT segment of the school lies within the domain of the school governing body.
2. The SGB shall put in place an IT Committee as a subcommittee of the SGB, to oversee governance responsibilities in respect of IT matters in the school.
3. The principal will have sitting on the IT committee, and the Committee will report to the SGB.
4. The SGB shall delegate to the principal (who may delegate further to appropriate members of staff) the day-to-day management of the IT segment of the school.

7 Involved Groups

Information Technology (IT) Governance at Rhenish Girls' High School shall involve the following groups:

7.1 The Governing Body (SGB)

1. The governing body is the entity with overall responsibility for IT Governance in the school.
2. It also provides coordination, alignment, and global oversight of IT policy, planning and compliance for the school.

7.2 The IT Committee

1. The IT Committee shall have exclusive responsibility to review and make recommendations to the Principal and SGB on all IT matters of the school.
2. The IT Committee shall consist of:
    a. An SGB member designated by the SGB as Chair of the Committee;

b. The Principal;

c. The senior member of the SMT responsible for academics or some other senior educator delegated by the principal to serve on the Committee;

d. The school's IT manager and/or senior IT educator;

e. At least two other people with the necessary knowledge, skills and/or interest, delegated/ invited/co-opted to serve on the Committee by the SGB;

f. One person with responsibilities and insights into the financial management of the school and its budgeting/expenditure/procurement processes.

7.3 The School's Senior Management Team (SMT)

1. The SMT shall assume overall responsibility for the implementation of IT policy, procedures, processes, procurement and the day-to-day management of IT in the school.
2. It shall further assume responsibility for advising the SGB on strategies, policies and practices that promote the effective use and management of IT to support the school's academic and administrative priorities.
3. The SMT will also be responsible for managing all aspects of Intellectual property security, both internally, in respect of the school's intellectual capital; and externally, with regard to copyright and the like.

8 Key Areas of Responsibility

1. The SGB shall take overall responsibility for:
    a. IT strategy and policy.
    b. Appropriate resourcing (human, structural, financial) of the IT provisioning in the school.
    c. Legal compliance structures.
    d. All contracts within the field of IT, both in terms of employment of SGB staff and entering into service-provider or procurement contracts.
2. The key areas of responsibility of the IT Committee shall include, but not necessarily be limited to:
    a. Creating effective lines of accountability, responsibility and authority for IT governance and compliance within the school.
    b. Monitoring and reporting to the SGB on the implementation of planned initiatives, projects, and ongoing IT services.
    c. Monitoring the stewardship of valuable or sensitive data or information in the possession of the school.

d. Ensuring that appropriate controls are in place to safeguard such information.

e. Monitoring the implementation of IT policies and alerting the SGB concerning instances of non-compliance.

f. Implementation and monitoring of legal compliance structures and policies.

g. Periodically reviewing the school's IT policies and recommending policy revisions, rescissions, and updates, as necessary.

h. Making annual recommendations to the SGB concerning the school's technology priorities, IT governance strategies, major IT projects and investment in IT.

i. Managing issues related to the flow of data, data coordination, data definitions, data ownership and authority

j. Addressing problems related to breaches of security, the discovery of disruptive technologies and the remediation of such breaches, as well as monitoring the progress of remediation on risk items related to IT, such as audit findings and other risks.

k. Resolving major resource conflicts or discord concerning competing priorities.

l. Monitoring the efficacy of the school's IT investments.

m. Arranging for and receiving periodic Independent assurances concerning legal compliance, risk management and policy relevance.

n. Recommending to the SGB strategic IT partnerships for the school.

o. In consultation with the Principal or Human Resources Committee, applying sanctions for non-compliance with IT governance, policies and procedures.

p. Addressing any other aspects of IT governance which may reasonably be assigned to the Committee by the SGB in the light of developments in the school or the IT field.

9 Prohibited activities or behaviour

9.1 The following activities and/or behaviour are prohibited:

3. Copying material bearing copyrights or patents, without proper licensing or authority
4. Using the school's information systems for political lobbying, personal gain or commercial purposes
5. Copying or removing software from the school's computers
6. Downloading material from the internet that is not related to official school activities or business
7. 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, governing body chairperson, headmistress or her delegated authorised representative.

8. 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.
9. 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, in accordance with the schools’ other policies.
10. Viewing or transmission of any material that violates any national, provincial or international law
11. Use of school information systems to gain unauthorised access to any system or data
12. 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.

9.2 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.

10 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 must 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 must 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.

10.1 Awareness Requirements

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

1. The approved social media sites may only be used for official purposes when using the school's information systems.
2. The message that the school wants to convey to other users must be clearly defined.
3. Postings must be kept legal, ethical and respectful.

4. 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 must refrain from engaging in any social media activities that may bring the school into disrepute, and will be held accountable for any such behaviour.
5. Personal details of educators, non-educators, learners and parents may not be disclosed. Educators, non-educators, learners and parents must 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.
6. 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.
7. 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.
8. All information that is published must be accurate, and confidential information may not be disclosed.
9. Copyright laws must be adhered to.
10. Only the official approved logo of the school may be used when participating in social media communication on behalf of the school.
11. Statements to the media must first be approved by the governing body or headmistress.
12. 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.
13. 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.

11 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.
5. Servers shall be backed up on a monthly basis by the IT service provider or the school's IT specialist.

12 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.

13 Sanctions

Refer to Annexure 1 for the process of response, and possible sanctions to be applied:

1. Failure to follow this policy or any other approved School policy on IT matters may result in disciplinary action, up to and including termination of employment of SGB employees, or referral to the Provincial Education Department in the case of state employees.

2. Any sanctions which may become necessary as a result of the breach of this or other IT-related policies will be determined by the principal, in consultation with the governing body chair and/or chair of the IT Committee and/or chair of a committee managing human resources and related matters in a school.

14 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

CBlabber

____

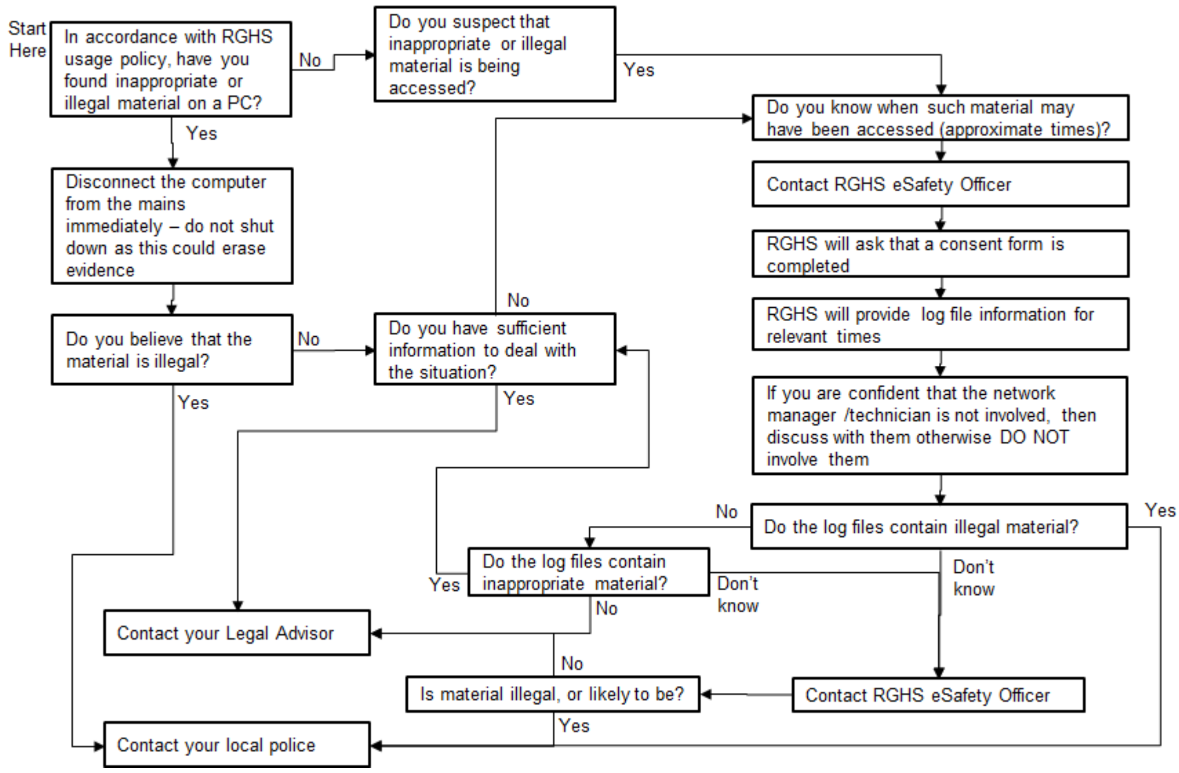
School principal

Annexure 1: Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse: If any apparent, or actual, misuse appears to involve illegal activity, for example,

1. Child sexual abuse images
2. Adult material which potentially breaches the Obscene Publications Act
3. Criminally racist material
4. Other criminal conduct, activity or materials

The RGHS flow chart below must be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


Start Here
In accordance with RGHS usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Do you know when such material may have been accessed (approximate times)?
Yes
Disconnect the computer from the mains immediately – do not shut down as this could erase evidence
Contact RGHS eSafety Officer
RGHS will ask that a consent form is completed
No
RGHS will provide log file information for relevant times
Do you believe that the material is illegal?
No
Do you have sufficient information to deal with the situation?
Yes
Yes
If you are confident that the network manager /technician is not involved, then discuss with them otherwise DO NOT involve them
No
Do the log files contain illegal material?
Yes
Do the log files contain inappropriate material?
Yes
Don't know
Don't know
No
Contact your Legal Advisor
No
Is material illegal, or likely to be?
Contact RGHS eSafety Officer
Yes
Contact your local police

The table below summarises the correct response to various incidents.

Students	Actions / Sanctions								
Incidents	Refer to class teacher / tutor	Refer to Head of Department / Head of KS/Head of House	Refer to Head Teacher/SMT	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal.			✓	✓		✓	✓		
Unauthorised use of non-educational sites during lessons	✓							✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓						✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓			✓	
Unauthorised downloading or uploading of files					✓		✓		
Allowing others to access school network by sharing username and passwords					✓		✓		
Attempting to access or accessing the school network, using another student's account					✓		✓		
Attempting to access or accessing the school network, using the account of a member of staff			✓		✓	✓	✓		
Corrupting or destroying the data of other users		✓							✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓	✓			✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓		✓	✓			✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓		✓	✓			
Using proxy sites or other means to subvert the school's filtering system					✓		✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓							
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓	✓		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓	✓					

Staff	**Actions / Sanctions**						
Incidents	Refer to line manager	Refer to Head Teacher/SMT	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓				✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓				✓		
Unauthorised downloading or uploading of files				✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓		✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓			✓		
Deliberate actions to breach data protection or network security rules		✓		✓	✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	✓	✓			✓		
Actions which could compromise the staff member's professional standing	✓	✓			✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓			✓		
Using proxy sites or other means to subvert the school's filtering system		✓		✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓		
Deliberately accessing or trying to access offensive or pornographic material		✓					✓
Breaching copyright or licensing regulations		✓	✓		✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓				✓

Annexure 2: General Considerations

Who needs to be involved?

In brief, everyone! E-safety is primarily a safeguarding issue, so anyone with responsibility for the welfare of children and young people needs to take responsibility for e-safety too. Children and young people themselves are integral to the process. They must be supported within an e-safe culture developed and maintained by both individuals and teams, both within an institution and beyond.

Responsibilities of children and young people

The responsibilities of children and young people themselves must not be underestimated – they are to be encouraged to develop their own sets of safe and responsible behaviours as, ultimately, this will provide the best defence for keeping them safe online. Responsibilities must be appropriate to the age, maturity and understanding of the child but, nevertheless, awareness must start at a very young age. Children and young people are encouraged to contribute to e-safety policies, for example, at student leader meetings. If children feel that their views and opinions have been considered, and can understand some of the issues affecting the decisions documented in the Student ICT Acceptable Use Policy (AUP), they may be more inclined to abide by them.

Key responsibilities for children and young people include:

1. Contributing to the development of e-safety policies.
2. Reading the policies – and adhering to them.
3. Taking responsibility for keeping themselves – and others – safe online.
4. Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
5. Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.
6. Respecting the feelings, rights, values and intellectual property of others.
7. Seeking help from a trusted person/adult if things go wrong, and supporting others who may be experiencing e-safety issues.
8. Discussing e-safety issues with parents and guardians in an open and honest way.

Responsibilities of the SMT team

The Senior Management Team (SMT) have statutory responsibilities for child protection, of which e-safety is an aspect. The SMT endeavour to have a sound awareness of e-safety issues, and to fully understand the importance of having effective e-safety policies and procedures in place. The leadership team ensure that e-safety implications are duly considered within all other school business.

E-Safety Safeguards

Refer to the RGHS Social Media and Social Networking Policy: All schools have a responsibility to ensure that all students and staff access the internet safely and responsibly. The following safeguards have been introduced into the school to help ensure all users remain safe on-line.

1. All users of the school network must sign an responsible use policy. Parents/guardians must also sign this policy.
2. The responsible use policy and E-Safety guidelines have been agreed by the School Governing Body and the School Management Team.

3. Staff have received E-Safety training.
4. Parents/Guardians‟ E-Safety evenings are held where current trends and risks are highlighted and key safety advice given.
5. The school‟s internet service is provided by Liquid Telecoms. RGHS provides filtering where inappropriate sites are blocked. These include pornography, race hate, drugs and violence.
6. Staff or students who find inappropriate websites must report them to the ICT technician/s who will then block the site.
7. All network users have their own usernames and passwords. It is emphasised that these must not be shared.
8. Activity on the network is monitored at all times by the technician/s. Individual use can be monitored, logged and reported if required.
9. Up-to-date anti-virus software and anti-spam detection and blocking packages are installed on the system and regularly updated by the technician/s.
10. The use of mobile phones to make calls or send texts is prohibited during lessons.
11. Teachers can be contacted by e-mail provided only the schools e-mail system is used. Students must not be talking to teachers using social networking sites. All social networking sites are filtered in school so that no access is possible.

Cyberbullying

Refer to the RGHS Social Media and Social Networking Policy: Cyberbullying is the use of Information Communications Technology (ICT), particularly mobile phones and the internet, to deliberately upset someone else. It differs from other forms of bullying in a number of ways:

1. **24/7 and the invasion of home / personal space.** It can take place at anytime, anywhere.
2. **Size of the audience.** Electronically circulated messages can reach a very large audience, very quickly. The spread of the messages is very hard to limit or control.
3. **Anonymity of the bully.** The bully may never be in the same physical space as their victim.
4. **The profile of the bully.** Age or size is not important. Bystanders can quickly become accessories to the bullying; for example, by passing on humiliating images.
5. **Cyberbullying can be unintentional.** It can be the result of not thinking or a lack of awareness of the consequences.
6. **Many cyberbullying incidents can themselves act as evidence.** This is one of the reasons why it is important to know how to respond.

Bullying is never acceptable. The school has a duty to protect all its members and provide a safe, healthy environment. Here are details about how an incidence of cyberbullying must be dealt with.

Cyberbullying Procedures

When dealing with any incident of cyberbullying it is important to follow the procedures set out in the schools' ICT & eSafety policy. However, there are some additional steps to take when responding to cyberbullying.

1. Reassure the victim that they have done the right thing and that everything will be done to deal with the problem.
2. Make sure the person knows not to retaliate or return any messages.
3. Help the person to keep any relevant evidence. Note down any web addresses used, take screen capture shots if possible and try to ensure messages are not deleted.
4. Advise the person of some simple steps they can take to prevent it from happening again. E.g. Blocking a contact, changing your own contact details, leaving a chat room, reporting the abuse to the service provider.

Action needs to be taken to contain the incident as quickly as possible.

1. Any on-line content must be removed.

2. Use disciplinary powers to confiscate any mobile phone being used for cyberbullying.
3. Ask the bully to tell you who they have sent messages on to.
4. In the case of any illegal content the Police must be contacted.

For a more detailed look at cyberbullying and ways of responding, the DCSF‟s publication „Safe to Learn: Embedding anti-bullying work in schools‟ provides some very useful guidance.

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school‟s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

1. **A planned e-safety lecture programme is provided – this covers both the use of ICT and new technologies in school and outside school**
2. **Key e-safety messages are reinforced as part of the planned programme of tutorial activities**
3. **Students must be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
4. Students must be helped to understand the need for the student ICT AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
5. Students must be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
6. Rules for use of ICT systems are addressed in the Responsible User Policy
7. Staff must act as good role models in their use of ICT, the internet and mobile devices

Education – parents / guardians

Many parents and guardians have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children‟s on-line experiences. Parents/guardians often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. The school will therefore seek to provide information and awareness to parents and guardians through: 1)Letters, newsletters, web site, 2) Information sessions to parents

1. **Curriculum E-safety must be a focus in all areas of the curriculum and staff must reinforce e-safety messages in the use of ICT across the curriculum.**
2. In lessons where internet use is pre-planned, it is best practice that students must be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
3. Where students are allowed to freely search the internet, using search engines, staff must be vigilant in monitoring the content of the websites the young people visit.
4. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, must be auditable, with clear reasons for the need.
5. Students must be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

6. Students must be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

1. An audit of the e-safety training needs of all staff will be carried out by Heads of Department. It is expected that some staff will identify e-safety as a training need within the Teacher Appraisal process.
2. All new staff must receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Responsible Use Policies
3. Key ICT staff will receive regular updates through attendance at RGHS information / training sessions and by reviewing guidance documents and others.
4. This E-Safety policy and its updates will be reviewed and consulted upon by staff .
5. Staff Input will provide advice / guidance / training to individuals as required.

Passwords

The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

1. Users can only access data to which they have right of access
2. No user must be able to access another‟s files, without permission (or as allowed for monitoring purposes within the school‟s policies).
3. Access to personal data is securely controlled
4. Logs are maintained of access by users and of their actions .

Responsibilities

The management of the password security policy will be the responsibility of the ICT Engineer. All users will be provided with a username and password by the Network manager who will keep an up to date record of users and their usernames. All users (adults and students) will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Passwords must contain a mix of letters and number, be a minimum of 6 characters long, contain upper and lower case characters. Through the Responsible Use Policy Statements all users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the Network Manager and will be reviewed, at least annually.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through staff meetings, briefings & Inset. Parent/guardians will be informed of the school‟s filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc. Any changes to the Filtering System must be supported by strong educational reasons for changes that are agreed. Users who gain access to, or have knowledge of others being able to access, sites which they feel must be filtered (or unfiltered) must report this in the first instance to the Network Manager who will decide whether to make school level changes.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment. Monitoring will take place as follows: Audit / Reporting Logs of filtering change controls and of filtering incidents will be kept by the Network Manager. On request, the filtering policy will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

1. When using digital images, staff must inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they must recognise the risks attached to publishing their own images on the internet eg on social networking sites.
2. Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images must only be taken on school equipment; the personal equipment of staff must not be used for such purposes.
3. Care must be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
4. **Students must not take, use, share, publish or distribute images of others without permission from a member of staff.**
5. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

6. **Written permission from parents or guardians will be obtained before photographs of students are published on the school website.**
7. **Student's work can only be published with the permission of the student and parents or guardians.**

Data Protection

Refer to the RGHS Data Protection Policy: Personal data will be recorded, processed, transferred and made available according to the Data Protection which states that personal data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Kept no longer than is necessary
6. Processed in accordance with the data subject‟s rights
7. Secure
8. Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, staff must ensure that they:

1. At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
2. Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
3. Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

1. The data must be encrypted and password protected
2. The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
3. The device must offer approved virus and malware checking software
4. The data must be securely deleted from the device, once it has been transferred or its use is complete.

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