Rhenish Girls'High School: Data Protection Policy

August 25

2020

This document represents the Rhenish Girls' High School Data Protection Policy

Data Protection Policy

Table of Contents

1. POLICY STATEMENT

1. Rhenish Girls' High School recognises that Personal Data Protection as per section 14 of the Constitution of the Republic of South African Act 1996 is an important piece of legislation to protect the rights of individuals in respect to any personal information that is kept about them, whether on computer or in manual filing systems. The additional acts including Protection of Personal Information Act (POPI/POPIA) and Promotion of Access to Information Act (PROATIA) are also considered.

2. Rhenish Girls' High School also acknowledge that from a regulatory perspective and for the confidence of Rhenish Girls' High School Learners, Parents & Educators, a Data Protection Policy will ensure that personal information given to Rhenish Girls' High School will be treated appropriately.

3. The policy acknowledges the right of access for individuals to information held about them and the right to stop or prevent processing likely to cause damage or distress and the right to compensation for unlawful processing. These rights apply to all data including CCTV images.

4. Rhenish Girls' High School is a Section 21 school and is registered at the Western Cape Education Department and the Department of Basic Education EMIS No.: 109310282.

5. The aim of this policy is to ensure Rhenish Girls' High School complies with this legislation and understands fully its obligations under the POPI Act.

6. This policy also aims to raise the awareness of the need to manage data in accordance with the Data Protection Principles listed below.

7. The Data Protection Policy is designed to consider the Promotion of Access to Information Act.

8. Rhenish Girls' High School's Lead Officer and named contact for Data Protection is the Vice Head Mistress.

9. There are also separate statements regarding the obligation and duties of the appointed roles, as defined in the Rhenish Girls' High School ICT and eSafety policies.

10. There are eight Principles of Data Protection contained in the Act which can be referred to by anyone who has a role to play in the management of personal information in Rhenish Girls' High School. These POPI principles are summarised below;

    a. The processing of information is limited which means that personal information must be obtained in a lawfully and fair manner.

b. The information can only be used for the specified purpose it was originally obtained for.

c. The Act limits the further processing of personal information. If the processing takes place for purposes beyond the original scope that was agreed to by the data subject, the processing is prohibited.

d. The person who processes the information must ensure the quality of the information by taking reasonable steps to ensure that the information is complete, not misleading, up to date and accurate.

e. The person processing the personal information should have a degree of openness. The data subject and the Information Regulator must be notified that data is being processed.

f. The person processing data must ensure that the proper security safeguards and measures to safeguard against loss, damage, destruction and unauthorised or unlawful access or processing of the information, has been put in place.

g. The data subject must be able to participate. The data subject must be able to access the personal information that a responsible party has on them and must be able to correct the information.

h. The person processing the data is accountable to ensure that the measures that give effect to these principles are complied with when processing personal information.

2. PRINCIPLES AND SCOPE OF POLICY

1. This policy applies to all personal information collected from all data subjects with whom the school interacts, including but not limited to parents, learners, educators, other staff members, contractors and other third parties who conclude any type of agreement or contract with the school.

2. Management, Learners, Parents, Educators, Employees, agency workers and contractors must be informed about data protection issues, and their rights to access their own personal data through the Induction process. SGB Members will receive guidance on Data Protection during their induction and any contractors and agency workers should be briefed on the importance of data protection at the start of their assignment, for example as it relates to safeguarding sensitive personal information on a school member, learner, contractor or guest.

3. Compliance with this policy is a condition of admittance at Rhenish Girls' High School and any deliberate breach of the policy may result in disciplinary action, which for serious or deliberate breaches may include dismissal. Knowingly breaching the provisions of POPI may also lead to legal action being taken against the organisation and individuals.

4. All data/information processed by Rhenish Girls' High School is covered by this policy.

5. A list of data protection definitions referred to in the Act and the Policy document is attached as Appendix 1.

3. KEY OPERATIONAL FRAMEWORK

1. For purposes of this policy, any references to data subjects include both potential and existing data subjects.

2. The type of information collected and processed will depend on the purpose for which it is collected, and any such information will be processed for that purpose alone. The school will inform the data subject of the information required, whether or not the supply of the information by that data subject is voluntary or mandatory, the purpose for which the information is to be processed, and the consequences of not providing the information. Processing of personal data will only be carried out where the data subject has given consent. This includes implied consent, for example where the data is necessary for the performance of:

    a. a contract to which the data subjects are a party; or

    b. for taking steps at the request of the data subject with a view to entering into a contract of employment or other legal obligation such as operating services or personal support services; or

    c. the processing is necessary for performing any obligation imposed by law on Rhenish Girls' High School in connection with support, service or employment; or

    d. the processing is necessary in order to protect the operation of services and vital interests of the data subject or another person in a case where (1) consent cannot be given by the individual; (2) Rhenish Girls' High School cannot be reasonably expected to obtain the consent or (3) in order to protect the vital interests of another person in a case where the consent by or on behalf of the data subject has been unreasonably withheld.

3. Details of the reasons why the data is sought and the reasons for which it will be used will be stated on all relevant Rhenish Girls' High School forms as outlined in Appendix 2(a).

4. The processing of sensitive personal data will only be carried out with the individual's explicit consent as outlined in Appendix 2(b). Sensitive personal data is defined at Appendix 1.

5. Data Received From Third Parties – Data which has been provided to Rhenish Girls' High School, in confidence, by a third party such as employment references or tenancy reports cannot normally be disclosed to the data subject, unless the author of the data (third party) can remain anonymous, agrees to its release at a later date or it is reasonable to comply with the access request without the originator's consent.

6. Where personal information is held by Rhenish Girls' High School on learners, parents, educators, contractors, employees and other individuals, these people have the right to access the information, unless it is exempt under the POPI.

7. Where a request for information is received (this must be in writing, including email correspondence), Rhenish Girls' High School will respond to the request within 40 days.

8. No charge will normally be made for requests for information. However Rhenish Girls' High School reserves the right to make a charge towards administration, stationery and postage costs where it is felt necessary to do so.

9. Rhenish Girls' High School is registered with the Western Cape Education Department. The Vice Head Mistress shall ensure subsequent requirements for learners, parents, educators, contractors, agents, and management registration are complied with and will liaise with the School Governing Body on the content of the registration.

10. Rhenish Girls' High Schools's Data Protection Policy can be found …… to which all authorised parties may request a copy via the Vice Head Mistress.

11. Rhenish Girls' High School allows audits for the School Management to undertake periodic reviews of the information being processed within their various departments.

12. Guidance and raising awareness on Data Protection issues, including the use of the Audit Procedures, can be obtained from the Vice Head Mistress. This can include;

    a. For New Learners, Parents, Educators, Management , Agents, Contractors and employees – Sensitisation to data privacy and protection will be provided at inductions arranged by the Vice Head Mistress as appropriate.

    b. Existing Learners and staff – Awareness sessions can be arranged for all employees by contacting the Vice Head Mistress. It is recommended that Data Protection is a subject that is discussed periodically at SGB Meetings.

    c. School Governing Body Members – can be provided with this policy and associated procedures on request. New members of the SGB are provided with awareness guidance as part of their induction process which should include guidance on Data Protection and Openness and Confidentiality.

13. The school will see to it that agreements are in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding of the protection of a data subject's personal information.

4. MONITORING AND REVIEW

1. On a pre-determined basis, each Head of Department must be provided with a copy of Rhenish Girls' High School's Data Protection Policy requesting that this be reviewed with any proposed amendments incorporated. This process must be prompted by the Vice Head Mistress. Any changes to Rhenish Girls' High School's policy will require the permission of the School Governing Body.

2. Any breaches of this policy or associated procedures will be reported to the School Management team in summary format together with details of the number of subject access requests and whether or not these access requests have been arranged within the time period set out by POPI.

3. This policy will be reviewed every 5 years from the date of implementation which will be the date the policy is approved by the School Governing Body, or earlier if deemed appropriate by changes to legislation.

5. PROCESSING AND USE OF PERSONAL INFORMATION

1. Personal information will be processed (a) lawfully, and (b) in a reasonable manner that does not infringe the privacy of the data subject.

2. A data subject's personal information will be used only for the purpose for which it was collected. The overall purpose of data collection, processing and use by the school is to ensure that the school is governed and managed in accordance with the principles and prescripts stipulated in the South African Schools Act and other applicable education legislation and policies.

3. Personal information may be processed only if these conditions are met:
    a. If the data subject consented to the processing of the personal information beforehand. Consent is obtained from parents/guardians through the signing of the applicable consent form at the beginning of the academic year. Where the data subject is a child, the consent must be given by a competent person.
    b. If processing is necessary to carry out actions in order to conclude or perform a contract to which the data subject is a party.
    c. If processing complies with a legal obligation imposed on the school.

d. If processing protects a legitimate interest of the data subject.
e. If processing is necessary for the school's proper exercising of a public law duty.
f. If processing is necessary for pursuing the legitimate interests of the school or a third party to whom the information is supplied.

4. Unless legislation provides for the processing of personal information, a data subject may object to such processing in terms of subparagraphs (d) to (f) above, in the prescribed manner and on reasonable grounds relating to the particular situation, in which case the school may no longer process the information.1

5. The school will not process personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject, unless processing is carried out with the data subject's consent or is necessary for the establishment, exercise or defence of a right or obligation in law, or the information has deliberately been made public by the data subject. The school may however process personal information concerning a learner's health or sex life if such processing is necessary to provide special support to learners or to make special arrangements in connection with their health or sex life.

6. DISCLOSURE OF PERSONAL INFORMATION

1. The information officer will refuse a third party's request for access to a record held by the school if its disclosure would involve the unreasonable disclosure of personal information about a data subject.

2. A data subject, having provided adequate proof of identity, has the right to request the school —
    a. to confirm whether or not it holds personal information about the data subject; and
    b. to supply the record or a description of the personal information so held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information. This request must be made within a reasonable time; at a prescribed fee, if any; in a reasonable manner and format, and in a form that is generally understandable.

3. A data subject may request the school to —
    a. correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
    b. destroy or delete a record of personal information about the data subject that the school is no longer authorised to retain.

[1] The prescribed objection forms are included in the Protection of Personal Information Act: Regulations relating to the Protection of Personal Information GN 42110 14 December 2018.

4. On receipt of a request, the school will, as soon as reasonably practicable —
    a. correct the information;
    b. destroy or delete the information; or
    c. provide the data subject, to his or her satisfaction, with credible evidence in support of the information.

5. The school will notify the data subject of the action taken as a result of the request.

7. SAFEGUARDING PERSONAL INFORMATION

1. The school is legally required to adequately protect personal information. Therefore, the school will continually review its security controls and processes to ensure that personal information is secure.

2. The following procedures are in place to protect personal information:
    a. Each new employee is required to sign an employment contract containing relevant consent clauses for the use and storage of employee information or any other action so required in terms of legislation, as well as an undertaking and agreement that (s)he will not, during or after the period of service to the school, convey any personal information of any data subject collected by the school to any third party.
    b. Every employee currently employed at the school is required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information or any other action so required in terms of legislation, as well as an undertaking and agreement that (s)he will not, during or after the period of service to the school, convey any personal information of any data subject collected by the school to any third party.
    c. Where feasible, all servers hosting personal information shall be located in a physically secure environment, where access is strictly controlled. All server rooms shall be regarded as high-risk security areas with strict access control.
    d. All servers shall be equipped and protected with approved antivirus software. The designated information technology (IT) service provider or the school’s IT specialist shall regularly install patch updates and upgrades.
    e. Only an authorised administrator shall be granted administrative rights to the servers. Administrative passwords shall be kept secret and changed on a regular basis, and only personnel nominated at the discretion of the executive committee of the governing body shall have access to the passwords.
    f. Third-party service providers will be required to sign a service provider agreement guaranteeing their commitment to the protection of personal information.

g. All electronic files or data are backed up by (insert option),2 which is also responsible for system security to protect against third-party access and physical threats. (Xxx)3 is responsible for electronic information security.
h. If the school has reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the school will notify the data subject of such breach in accordance with sections 22(4) and (5) of POPIA.

8. RESPONSIBILITIES FOR COMPLIANCE

1. The Vice Head Mistress is responsible for the following:
    a. Notification and registering this policy with the WCED
    b. Coordinating any amendments to Rhenish Girls' High School's registration
    c. Monitoring and reporting to the School Governing Body on compliance and any subject access rights or requests
    d. Advising Heads of Departments on audit procedures
    e. Advising Heads of Departments on Data Protection
    f. Liaising with the Governing Body members on Rhenish Girls' High School's Data Protection Policy and any queries arising
    g. Liaising with the ICT Department members on matters relating to IT Security
    h. Liaison with the WCED and designated officers as required, for example where there is a breach of data protection principles

2. The Vice Head Mistress is responsible for ensuring that storage of digital data, systems back up, storage and disposal of digital media and ICT systems are secure and that all associated ICT Policies and Procedures underpin and align with this Policy.

3. The Vice Head Mistress is responsible for authorising actual data collection activities.

4. The Vice Head Mistress will assist in implementing the requirements of the POPI by:
    a. Providing advice and support to all departments on matters relating to compliance with POPI
    b. Disseminating information relating to the POPI to those with Data Protection responsibilities

[2] See the FEDSAS information letter on the options available.
[3] This is the responsibility of either an external service provider contracted by the school for this purpose, or an employee to whom this function has been delegated. This delegation must be in writing, and must set out the precise scope of duties.

c. Responding and co-ordinating requests from individuals to access personal information we hold about them, whether they be employees (past/present) or learners, parents, educators, management, service users or contractors

5. Each Heads of Department has specific responsibilities for safeguarding the personal and sensitive information held on data subjects within their portfolio and complying with the provisions of this policy and POPI.

6. It is the individual responsibility of each learner, parent, educator, management member and School Governing Body Member to ensure they comply with Rhenish Girls' High School's Data Protection policy and these associated procedures.

9. SECURITY OF DATA (RETENTION AND DISPOSAL)

1. All staff are responsible for ensuring that any personal data which is held in their department is kept securely and that they are not disclosed to any unauthorised third party.

2. All personal data must be accessible only to those who need to use it. Judgement should be based upon the sensitivity and value of the information in question; but always consider keeping personal data:
    a. in a lockable room with controlled access
    b. in a locked drawer or filing cabinet
    c. if data is computerised then it should be stored on Network servers and not on local systems and have suitable security access levels applied.
    d. particular care should be taken of portable ICT equipment, memory sticks, etc which should be password protected to prevent unauthorised access. Where sensitive personal data is by necessity stored on memory sticks these must be protected by Advanced Encryption Standard encryption and passwords strictly controlled by the Vice Head Mistress.
    e. sensitive personal data should not be kept on memory sticks or routinely taken from Rhenish Girls' High School premises on any form of removable media without the necessary precautions being exercised.
    f. Data held on removable media (CD/DVD/flash drives/memory sticks/ removable hard drives) must be disposed of in accordance with acceptable data disposal methods.

3. Care must be taken to ensure that PC monitors and Mobile Device Screens are not visible except to authorised staff and that computer passwords are kept confidential. PC's, Mobile Phones, Tablets, NetBooks and Laptops should not be left unattended without password protected screen savers and manual records should not be left where they can be accessed by unauthorised personnel. Educators and staff are encouraged to operate a "clear desk" policy when finishing work each day.

4. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste".

5. This policy also applies to educators and management who process personal data outside Rhenish Girls' High School premises, such as when working from home. Off-site processing presents a potentially greater risk of loss, theft, damage to personal data. Staff should take particular care when processing personal data at home or in other locations. Any loss of data from either Rhenish Girls' High School premises or off site must be reported to the Vice Head Mistress immediately.

5.6 **Retention & Disposal**

1. Records of personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless —
    a. retention of the record is required or authorised by law;
    b. the responsible party reasonably requires the record for lawful purposes relating to its functions or activities;
    c. retention of the record is required by a contract between the parties thereto; or
    d. the data subject or, where the data subject is a child, a competent person has consented to the retention of the record.

2. The school will destroy, delete or de-identify a record of personal information as soon as is reasonably practicable after the school is no longer authorised to retain the record. This will be done in a manner that prevents reconstruction of the information in an intelligible form.

3. See Appendix 4 for a list of prescribed retention periods.

4. The school will restrict the processing of personal information in accordance with section 14(6) of POPIA.

10. CLOSED CIRCUIT TELEVISION (CCTV)

1. Rhenish Girls' High School has a requirement for maintaining security through the use of closed circuit television systems.

2. Where CCTV is in use, images are treated as "data" in the same manner as paper or computer based information. The main purpose of collecting data from CCTV cameras is the protection of Rhenish Girls' High School tenants, residents, service users, employees and the

public, the prevention of crime or anti-social behaviour and to safeguard Rhenish Girls' High School property. Data from CCTV cameras may be used as evidence during criminal or other legal proceedings and may be passed to other agencies within the scope of the Security function.

3. The number and type of cameras is also carefully considered. Learners, parents, educators, visitors and employees should not feel uncomfortable by the presence of CCTV and it is not used to monitor private areas such as inside a bedroom or bathroom. It should also be noted that cameras may not always be immediately visible to the casual observer.

4. Management consultation on any new camera installations includes discussing if there are alternative options, any underlying reasons why the need for CCTV has arisen, the number and positioning of cameras, secure image recording and storage facilities, who has access to recorded images and whether the system is temporary, permanent or subject to a period of review.

11. MONITORING AND RECORDING

1. Systems in use at Rhenish Girls' High School are monitored on a constant basis. Designated staff check the systems constantly, for example to what is happening along the entrances and boundaries. Staff should not use the system for monitoring movements of people in and around the school. They are not be expected to respond to requests from various individuals (a parent for example) who, may want to find out what time someone went out or came back into the school.

2. The CCTV monitors may not be in a position where images can be seen by members of the public. The CCTV monitors should be shielded if there is a risk that unauthorised people would be able to view images on screen.

3. Images will be recorded on a time loop. This means that recorded images are not kept indefinitely and will be recorded over on a regular basis. Usually this period is around one month or as long as is believed necessary by school management to ensure the appropriate levels of safety at the school. The length of time images are stored before being overwritten is known to employees responsible for monitoring the system in order to respond to enquiries from authorised parties.

4. Recorded images are kept securely and staff may not access these without the permission of the Vice Head Mistress and only for specific purposes related to the use of CCTV, i.e. crime prevention/detection or dealing with anti-social behaviour.

5. CCTV images are the property of Rhenish Girls' High School as the Data Controller.

12. NOTIFICATION

1. It is the responsibility of Rhenish Girls' High School, through the Vice Head Mistress (Reactive), to ensure that proper warning signs are sited at the school entrance, notifying that selected areas of the school are monitored by CCTV.

13. Details of information officer

INFORMATION OFFICER DETAILS

Name: _____

Telephone number: _____

Fax number: _____

E-mail address: _____

DEPUTY INFORMATION OFFICER DETAILS

Name: _____

Telephone number: _____

Fax number: _____

E-mail address: _____

SCHOOL OFFICE DETAILS

Telephone number: _____

Fax number: _____

Postal address:

Physical address:

E-mail address: _____

Website:

14. Access to documents held by the school

1. Any request for access to a document held by the school must be dealt with in accordance with the school's manual in terms of the POPIA, which contains the prescribed forms as well as details of prescribed fees. This manual is available from the school principal or the school's website, www.rhenish.co.za

15. Policy amendments

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

SIGNED AT ____Stellenbosch_____ON THIS __30_____ DAY OF_____November 2020_____

Governing Body Chair

16. APPENDIX 1: DATA PROTECTION DEFINITIONS USED IN THIS POLICY

For purposes of this policy, the following terms are assigned the meanings as indicated:

"Biometric information" means information obtained through a technique of personal identification that is based on physical, physiological or behavioural characterisation, including blood-typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

"Competent person" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

"Data subject" means the person to whom personal information relates.

Data Controller – a person or organisation who decides how personal data is to be processed and for what purpose. Rhenish Girls' High School is the data controller, not individual staff members.
"Deputy information officer" is the vice-principal.[4]

"Employee" refers to a staff member appointed at the school in terms of sections 20(4) and (5) of the South African Schools Act 84 of 1996.

"Employer" refers to (*school*).

"Information officer" is the school principal.

"Personal information" means information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person, including but not limited to —

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

[4] Section 56 of POPIA provides that deputy information officers may be "designated" to perform the duties of the information officer. FEDSAS recommends that the vice-principal be designated as such.

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person, or if the disclosure of the name itself would reveal information about the person.

''Processing'' means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including —

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use thereof;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

''Record'' means any recorded information —

(a) regardless its form or medium, including any of the following:

(i) Writing on any material

(ii) Information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored

(iii) A label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means

(iv) A book, map, plan, graph or drawing

(v) A photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence.

''Responsible party'' means the governing body of (*school*), who determines the purpose of and means for processing personal information.

Data (including manual data/relevant filing system) – information which:
a) is being processed by means of equipment operating automatically in response to instruction given for that purpose, such as information in the internet access channels,
b) is recorded with the intention that it should be processed by means of such equipment;
c) is recorded as part (or with the intention that it should form part) of a relevant filing system (i.e. any set of information relating to individuals to the extent that, although not processed as in (a) above, the set is structured, whether by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible); and
d) does not fall within paragraph a), b), or c) but forms part of an accessible record as defined in Section 68 of the DPA.

Examples of manual data that may qualify as structured manual files:
• Personnel Files – applications forms, appraisal forms, disciplinary records, sickness records, supervision notes etc;
• School Applicaiton Records – application forms, waiting lists, accounts etc; and
• Card indices – lists of names and addresses, contact numbers etc.

Personal Data

– all data relating to a living individual who can be identified from that data. This includes any expressions of opinion about that individual as well as any intentions that any person has regarding that individual.

Sensitive Personal Data

– includes the following:
• Racial or ethnic origin;
• Political opinions;
• Religious or similar beliefs;
• Financial Information;
• Mental or physical health;
• Family details;
• Criminal records or allegations of criminal conduct.

Processing

the management of data or information includes obtaining, recording, holding, organising, adapting consulting, retrieving or otherwise performing some operation on it. Processing also includes disclosure of data and destroying data or information. Almost all uses of data or information are included in the definition of processing.

17. APPENDIX 2: Rhenish Girls' High School'S DATA PROTECTION STATEMENT

The statement below may be added to Rhenish Girls' High School forms or documents as necessary to comply with POPI.

"Rhenish Girls' High School is registered under POPI (1996) with the Western Cape Education Department. Rhenish Girls' High School is the Data Controller for the purposes of the Data Protection Act.

The information you provide will be treated in confidence and in compliance with the Act. We may pass the information to other agencies or organisations as allowed by the law. As the Data Subject you have the right to access the information we hold on you. If you wish to exercise this right please contact our office in writing or via email with the details of your request."

18. APPENDIX 3: SUBJECT ACCESS REQUEST FOR PERSONAL DATA

Has the data subject made a request in writing and paid the required fee (if required)?
YES
NO
No obligation to disclose
Has the person requesting the data satisfied you that she/he is the data subject?
NO
No obligation to disclose until their identity is confirmed
YES
Will disclosure of personal data require you to disclose personal data of a third party in order to comply with request?
YES
Normally no obligation to disclose that part of the personal data relating to the third party unless third party consents or it is reasonable to dispense with consent.
NO
Rhenish Girls' High School must provide requested information promptly and in any event within 40 days

19. APPENDIX 4: RETENTION OF Rhenish Girls' High School RECORDS

Rhenish Girls' High School processes personal data on a number of different subjects; these include New Learners, Parents, Educators, Management , Agents, Contractors and employees

We will ensure that all data is processed in accordance with the principles of Data Protection and will be retained securely for as long as it is required. Sensitive Personal Data, for example resident's family records or a tenant's financial circumstances, will be kept in recognised secure filing systems with controlled access. All sensitive data processed by Rhenish Girls' High School, under the definition in Appendix 1 of this Policy is listed below with retention period and storage criteria. Other information, for example minutes of Committee meetings, which falls under Schools Act is omitted from this Appendix.

We will comply with legislation and good practice advice wherever possible to ensure that data is kept only for as long as it is legally required and is securely destroyed thereafter.

Table 1 (4) **Data Type**	**Department**	**Retention Period (Yrs) & Reference**	**Storage**
Learners Files	Department and Grade Heads	While active	Locked cabinet/cupboard
Former Learners Files	Department and Grade Heads	6 Years from date of leaving	Locked cabinet/cupboard
Medication Records	Hostel & Secretary	3 Years (CC Guidance 3/09)	Locked cabinet
School Performance Records	Department and Grade Heads	While active	Locked cabinet/cupboard
User Access Data	ICT	1 Year	Computer Server
Internet Usage Records	ICT	3 Years	Computer Server
Applicant Data (Waiting List)	Administration	While active	Locked cabinet/cupboard
Former Applicants	Administration	1 Year	Locked cabinet/cupboard
Educator Records	Administration	While active	Locked cabinet/cupboard
Former Educator Files	Administration	3 Years	Locked cabinet/cupboard
Employment Files incl Attendance records	Administration	6 years (CIPD)	Locked cabinet/cupboard

Prescribed retention periods for personal information

Compensation for Occupational Injuries and Diseases Act (COIDA) 130 of 1993

Sections 81(1) and (2) of COIDA require a retention period of four years from the last date of entry for the following documents:

- A register, record or reproduction of the earnings and other prescribed particulars of all employees

Occupational Health and Safety Act (OHSA) 85 of 1993

Where health and safety committees have been established in terms of section 20(2) of OHSA, these committees' recommendations to the school on issues affecting employee health and any report submitted to an inspector in terms of such recommendations must be kept for three years.

Moreover, records of incidents reported at work must be kept for three years, as determined by regulation 9 of the General Administrative Regulations, 2003, promulgated under OHSA.

Basic Conditions of Employment Act (BCEA) 75 of 1997

The BCEA requires a retention period of three years from the last date of entry for the following documents:

- Written particulars of an employee after termination of employment (section 29(4))

- Employee's name and position

- Time worked by each employee

- Remuneration paid to each employee (section 31)

Employment Equity Act (EEA) 55 of 1998 (if applicable)[5]

Section 26 of the EEA and regulation 3(2) of the General Administrative Regulations, 2009, promulgated under the EEA require a retention period of two years for the following documents:

- Records in respect of the school's workforce, employment equity plan and other records relevant to compliance with the EEA

In addition, regulation 4(11) requires a retention period of two years for the report that is sent to the Director-General, as prescribed in section 21 of the EEA.

Labour Relations Act (LRA) 66 of 1995

In terms of section 205(1) of the LRA, the school must retain the following records, in their original form or a reproduced form, for a period of three years from the date of the event or the end of the period to which they relate:

- Records that an employer is required to keep in compliance with any applicable collective agreement or arbitration award

In terms of section 205(3) of the LRA and section 5 of schedule 8 to the LRA, the following documents must be retained for an indefinite period:

[5] See the FEDSAS legal opinion "Employment equity and public schools" to establish whether or not these prescripts apply.

- Prescribed details of any strike, lock-out or protest action involving the school's employees

- Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer, and the reasons for the actions

Unemployment Insurance Act 63 of 2002

Section 56(2)(c) of the act requires that the following documents be retained for a period of five years from the date of submission:

- Personal records of each current employee, including names, identification numbers, monthly remuneration, and work address

Income Tax Act 58 of 1962

In terms of paragraph 14(1)(a) to (d) of schedule 4 to the Income Tax Act, the school must retain records showing the following, for a period of five years from the date of submission in respect of each employee:

- The amount of remuneration paid or due to the employee
- The amount of employees' tax deducted or withheld from the remuneration paid or due
- The income tax reference number of that employee
- Any further prescribed information
- The employer's reconciliation return

Department of Basic Education: National Protocol for Assessment Grades R–12

According to paragraph 28(11) of the national protocol, the school must retain a learner's profile for a period of three years after the learner has passed Grade 12 or exited the schooling system for any reason whatsoever, after which it should be destroyed.

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