RUSTENBURG GIRLS' HIGH SCHOOL

PROTECTION OF INFORMATION POLICY

1. PURPOSE OF THIS POLICY

Rustenburg Girls' High School (**the School**), its School Governing Body (**the SGB**) and its Staff recognise the need to protect the information held by the School, as laid out in the Protection of Personal Information Act, no 4 of 2013 (**POPIA**). In addition, the following laws also bear relevance to the storage and protection of personal information - Provincial Archives and Records Services Act (no 3 of 2005) and National Archives and Record Service of South Africa Act (no43 of 1996); Electronic Communications and Transaction Act (no 25 of 2002); Promotion of Access to Information Act (no 2 of 2000). The purpose of this policy, therefore, is:

a. To outline the measures taken to safeguard the personal information held by the School from threats, whether internally or externally, deliberate or accidental and thus protecting the right of privacy of all data subjects (people or organisations for whom the school collects and stores data, as listed in **Appendix A** of this policy).
b. To indicate how we protect the School's records and information as listed in **Appendix A** in order to ensure the continuation of the day to day running of the School.
c. To regulate the manner in which personal information is processed by the School.
d. To regulate the length of time for which personal information is retained by the School (see **Appendix B**)
e. To establish an Information Officer (see **Appendix C**) to ensure respect for and to promote, enforce and fulfil the rights of data subjects referred to in **Appendix A**

2. INTRODUCTION AND BACKGROUND

POPIA seeks to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise the personal information that they hold in any way. In addition, the Regulations relating to the Protection of Personal Information, 2018 (**POPI Regulations**), require the Information Officer to develop, implement, monitor and maintain a compliance framework to ensure compliance with the POPIA.

More detail in regards to Compliance Frameworks is attached as **Appendix D**

3. SCOPE

The SGB and the Principal of the School are ultimately responsible for ensuring that information security is properly managed. The Information Officer and Deputy Information Officer, are responsible for (see **Appendix C** for more detail):

a. The development and upkeep of this policy.
b. Ensuring this policy is supported by appropriate documentation, such as procedural instructions.
c. Ensuring that documentation is relevant and kept up to date.
d. Ensuring this policy and subsequent updates are communicated to the SGB and staff where applicable.

The Information Officers and all members of staff are responsible for adhering to this policy, and for reporting any security breaches or incidents to the Information Officers.

4. PRINCIPLES

The Information Officers, Operators (as defined by the Act) and staff of the School are committed to the following principles:

a. To be transparent with regards to the operating procedures governing the collection and processing of personal information.
b. To comply with all applicable regulatory requirements regarding the collection and processing of personal information.
c. To collect personal information only by lawful means, with consent, and to process personal information in a manner compatible with the purpose for which it was collected.
d. Where required by regulatory provisions, to inform individuals when personal information is collected about them.
e. To treat sensitive personal information that is collected or processed with the highest care as prescribed by regulation.
f. Where required by regulatory provisions or guidelines, to obtain individuals' consent to process their personal information.
g. To strive to keep personal information accurate, complete and up to date and reliable for their intended use.
h. To develop reasonable security safeguards against risks such as loss, unauthorized access, destruction, abuse, amendment or disclosure of personal information.

i. To provide individuals with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or delete personal information.
j. To share personal information, by permitting access, transmission or publication, with third parties only with the express permission of the subject, and with a reasonable assurance that the recipient has suitable privacy and security protection controls in place regarding personal information.
k. To comply with any restriction and/or requirement that applies to the transfer of personal information internationally.

5. MONITORING

The SGB, the Principal, Information Officer (**Appendix C**) and all operators, as defined by the Act, of the School are responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, operating procedures, notices, consents and appropriate related documents and processes. Periodic reviews and audits will be conducted where appropriate, to demonstrate compliance with privacy regulation, policy and guidelines.

6. OPERATING CONTROLS

The School shall establish appropriate privacy operating controls that are consistent with this policy and regulatory requirements. This will include:

a. Allocation of information security responsibilities.
b. Incident reporting and management.
c. User ID addition, removal and authentication control.
d. Information security training and education.
e. Data creation, classification, backup, retrieval and disposal.
f. Disaster recovery.

7. IMPLEMENTATION

a. This policy is implemented by the School will be adhered to by all staff who are tasked with collecting and processing of personal information.
b. Non-compliance with this policy may result in disciplinary action and possible termination of employment or mandate, where applicable.
c. This policy explains how we obtain, use and disclose personal information, as is required by POPIA.

d. The School is committed to protecting the privacy of pupils, parents, staff and suppliers, and to ensuring that any personal information is collected and used properly, lawfully and transparently.

8. PERSONAL INFORMATION COLLECTED

The information collected and held by the school on various categories of data subject is spelled out in **Appendix A** below, although this list should not be considered exhaustive. The type of information held depends on the need for which it is collected and will be collected for that purpose only. Whenever possible, we will inform the subject what information they are required to provide us with and what information is optional.

9. HOW PERSONAL INFORMATION IS USED

Personal information gathered and held by the School will only be used for the purposes for which it was gathered.

10. DISCLOSURE OF PERSONAL INFORMATION

Personal information gathered and held by the School will only be disclosed to a third-party with the express permission of the subject, unless the School is required to do so by the South African Schools Act or other relevant legislation, or where it may be necessary to protect our rights.

11. SAFEGUARDING PERSONAL INFORMATION

a. It is a requirement of POPIA to adequately protect the Personal Information held by the School and to avoid unauthorised access and use of such information. The School undertakes to continuously review our security controls and processes to ensure that the Personal Information we hold is secure.
b. Current control measures include:
    i. All employees involved in collection, capture, processing and disclosure of subject data have been informed as to their responsibilities under the Act and required to sign an addendum to their contract of employment stating that they understand these responsibilities.
    ii. The primary storage location of a subject's electronic data is a secure server, physically held in a locked and alarmed area of the School. This server is backed-up regularly and automatically, both locally to a physically separate server, in a location which itself is locked and alarmed, as well as remotely to a server held off-site in a secure location by one of our service providers.

iii. Disaster recovery procedures are in place and are tested regularly.
iv. Information held in hard-copy form (e.g. application forms) is filed in storage facilities in the Administration offices at the School's premises in **Campground Road, Rondebosch**. These offices are locked and alarmed when no member of staff is present.
v. Employees only have access to the subject data required for them to perform their duties as laid out in their contract of employment. This access is controlled by password-managed privileges and access control within the School's main Information Systems.
vi. The Information Officer and Deputy Information Officer (**Appendix C**) are responsible for the compliance with the conditions of the lawful processing of Personal Information and other provisions of POPIA.
vii. No data is sent off-site for processing by third parties on the school's behalf without the explicit permission of the data subjects. Where specialist third-party processing is done on site, it is done under the supervision of an authorised member of School staff.
viii. As the School is a Google school, there may be occasional usage of Google Drive for the storing of incidental personal information on a temporary basis (e.g. classlists or marksheets). This will never be the primary storage medium for personal information (see 11. b. ii. above) and such information will be deleted as soon as possible.

12. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

a. Data subjects have the right to access the Personal Information the School holds about them, as well as the right to ask us to update, correct or delete their Personal Information on reasonable grounds.
b. Once a data subject objects to the processing of their Personal Information, the School will no longer process said this information, unless required to do so in the performance of our statutory duties under the South African Schools' Act or other legislation.
c. The School will take reasonable steps to confirm a data subject's identity before providing details of their Personal Information or making changes to their Personal Information.
d. All data subjects are contacted annually (as far as is reasonably possible), sent a copy of the data held on them by the School, and invited to correct this information or add to it as appropriate.

13. DISPOSAL OF PERSONAL INFORMATION

a. Documents/electronic information may be deleted/destroyed at the end of the required retention period as specified in law or when they are no longer required for the purpose for which they were collected. The Information Officer will request departments to attend to the destruction of their documents/ information and these requests shall be attended to as soon as possible.
b. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the files. Original documents must be returned to the owner thereof, failing which, they should be retained by the School pending such return.
c. Methods of deletion/destruction to be specified
d. The minimum retention period for each class of information is listed in **Appendix B** below.

14. AMENDMENTS TO THIS POLICY

Amendments to this Policy will take place on an ad hoc basis, and it will be reviewed annually.

15. DOCUMENT CONTROL

DATE	DESCRIPTION
June 2018	Initial DRAFT Document
June 2019	Final DRAFT Document
March 2020	APPROVED
January 2021	Revised following review by SEESA to align with requirements of POPIA

APPENDIX A: PERSONAL INFORMATION AND RECORDS HELD BY THE SCHOOL OF THE FOLLOWING DATA SUBJECTS

1) LEARNERS – as defined by the South African Schools Act NO 84 OF 1996

    a. Learner's application for admission to a public school indicating the following personal information:
        i. Name and Surname of the learner
        ii. ID number of the learners
        iii. Date of Birth
        iv. Gender
        v. Race
        vi. Physical address and contact details
    b. Supporting documents as follows
        i. Birth certificates
        ii. ID documents
        iii. Inoculation certificate
        iv. Report cards from previous school
        v. Study and asylum permits
    c. Learner profiles
    d. Disciplinary hearings
    e. Promotion and assessment records
    f. Extra and Co-curricular records
    g. Behavioural records
    h. Photographs of learners
    i. Biometrics of learners

2) PARENTS - as defined by the South African Schools Act NO 84 OF 1996

    a. ID documents of parents
    b. Personal Information of parents
        i. Name and Surname
        ii. Date of birth and ID number
        iii. Gender
        iv. Race
        v. Marital status
        vi. Medical Aid
        vii. Home and work physical and postal address
        viii. Landline and mobile telephone numbers
        ix. Home and work email address
        x. Profession and Employment details
        xi. Names of all the children in the family
    c. Financial record of school fee account
        i. Ledger account
        ii. Statement of account
        iii. Receipts
        iv. Journal entries
    d. Application for exemption of school fees with the following supporting documents
        i. Proof of Income
        ii. Bank Statements
        iii. Other Financial documents proving income of parent
        iv. Documentation proving other children in the family
    e. Correspondence with parents

3) EMPLOYEES EMPLOYED BY THE SCHOOL

a. Personal information of all employees
    i. ID documents
    ii. Personal contact details
    iii. Qualification certificates
    iv. Banking details
    v. Registration with statutory bodies SARS, UIF, Skills development, Workman's compensation
    vi. Registration with SACE
    vii. Curriculum Vitae
    viii. References
    ix. Job Description
    x. Performance appraisals
    xi. Contract of employment
    xii. Attendance registers
    xiii. Medical records
    xiv. Leave application forms
    xv. Payroll administration records
    xvi. Correspondence
    xvii. Disciplinary hearings
    xviii. Biometrics of employees
    xix. Police clearance certificate
    xx. Driver's license – Professional Driving permits
    xxi. Photographs
b. Personal Information of prospective employees
    i. Interview scores
    ii. CV and supporting documents
c. Personal information past employees
    i. Documents as listed above in (a)

4) EMPLOYEES EMPLOYED BY THE STATE

a. Personal information
    i. ID documents
    ii. Personal contact details
    iii. Qualification certificates
    iv. Salary scales
    v. Banking details
    vi. Registration with SACE
    vii. Curriculum Vitae
    viii. References
    ix. Performance appraisals
    x. Attendance registers
    xi. Medical records
    xii. Leave application forms
    xiii. Pay slips issued by District
    xiv. Correspondence
    xv. Disciplinary hearings
b. Personal Information of prospective employees
    i. Interview scores
    ii. CV and supporting documents
    iii. SGB recommendations

c. Personal information past employees
    i. Documents as listed above in (a)

5) LEARNERSHIPS

a. Personal information of all student teachers on learnership contracts
b. ID documents
c. Contact details
d. Contract agreement
e. Performance appraisals
f. Banking details
g. Pay slips
h. Correspondence

6) TEMPORARY STAFF – Coaches, Educators, Invigilators, Administrators

a. Personal information
b. ID documents
c. CV and references
d. Contact details
e. Contract agreement
f. Banking details
g. Payroll records - Payslips
h. Correspondence

7) SUPPLIERS

a. Personal information of all suppliers
b. Financial records of all suppliers account
c. Contract agreement with all suppliers
d. Correspondence with all suppliers
e. Tender documents

8) GOVERNING BODY and SUBCOMMITTEES

a. Personal information of all members
b. Contact details
c. Code of conduct of SGB
d. Minutes of all meetings

9) TENANTS

a. Personal Information details
b. Lease agreements
c. Correspondence

10) DEPARTMENT OF EDUCATION

a. Legislation – Acts, Regulations
b. Circulars
c. Curriculum assessment documents
d. Whole school evaluation records
e. Post establishment records
f. Norms and Standards Allocation records

g. Compensation for exemption records
h. Snap survey records
i. Section 38A applications
j. Approval application to open an Investment account.
k. Approval to obtain loan, extend, lease etc.
l. Correspondence

11) PAST LEARNERS

a. Personal Information details
b. Contact details
c. Correspondence

12) SPONSORS

a. Personal Information details
b. Contact details
c. Receipts – 18A
d. Donation Register
e. Correspondence

13) ADVERTISERS

a. Personal Information details
b. Contact details
c. Details of advert
d. Correspondence

14) SPORTING BODIES

a. Personal Information details
b. Contact details
c. Subscriptions
d. Correspondence

15) ACADEMIC AUTHORITIES – SAQA, UMALUSI, SACE, IEB

a. Personal Information details
b. Contact details
c. Subscriptions
d. Correspondence

16) SGB ASSOCIATIONS – FEDSAS, GBF

a. Personal Information details
b. Contact details
c. Newsletters
d. Subscriptions
e. Correspondence

17) UNIONS – NAPTOSA, SAOU, SATU

a. Personal Information details
b. Contact details

c. Subscriptions
d. Correspondence

18) STATUTORY BODIES – SARS, Department of Labour, SETAs

a. Personal Information details
b. Contact details
c. Statutory returns
d. Correspondence

19) SCHOOL AUDITORS

a. Personal Information details
b. Contact details
c. Certificates of their registration with an authorizing body
d. Audit reports
e. Contract of service
f. Statement of account
g. Financial statements
h. Correspondence

20) INSURANCE HOUSES

a. Personal Information details
b. Contact details
c. Insurance agreement
d. Claim forms
e. Correspondence

21) BANKING INSTITUTIONS

a. Personal Information details
b. Contact details
c. Record of accounts kept at the institution
d. Correspondence

22) ATTORNEYS / DEBT COLLECTORS

a. Personal Information details
b. Contact details
c. Records of case referred to them
d. Contract entered into with 3rd party
e. Their account
f. Correspondence

23) OUTSOURCED SERVICES

a. Personal information details of company
b. Contact details
c. Contract with company
d. Statement of account
e. Correspondence

24) TRUSTEES

a. Personal information details of each trustee
b. ID documents of each trustee
c. Trust documents
d. Minutes of meetings
e. Correspondence

25) HOSTEL RECORDS

a. Personal information of each staff member
b. Contact details of each staff member
c. Lease agreements of staff living of premises
d. Duty schedule and roster
e. Personal information of all learners and their parents
f. Financial records
g. Incident records
h. Correspondence

26) EDUCATIONAL INSTITUTIONS (Public-Independent Schools or Universities)

a. Personal information of institution
b. Contact details
c. Correspondence

27) SCHOOL RECORDS

a. Constitution
b. Strategic Plan – Development Plan and Improvement Plan
c. School Policies
d. Financial records
    i. Financial Ledgers and books of first entry
    ii. Budgets
    iii. Financial statements
    iv. Reports on Financial matters
    v. Bank statements and records
    vi. Details of all investment accounts
    vii. Payroll records
    viii. List of all assets and inventory
e. Incident Records
f. Curriculum documentation
g. Learner Assessment records
h. Lease agreements & Contracts
i. Minutes of meetings
j. LTSM records
k. School Magazines
l. Organogram of school staff
m. Software programmes
    i. Pastel Accounting
    ii. Payroll software (VIP)
    iii. Administrative software (Engage, Pencilbox, etc.)
    iv. Library programmes (LIBWIN)
    v. Backups of all records
n. Internal forms
o. Correspondence

Appendix B:

Class of Information	Held By?	How Held?	How long?
Learners	Operations	Engage	While a pupil at the school (Academic record = indefinite)
Parents	Operations	Engage	While child is a pupil of the school
School Employees	Finance/ Operations	Engage/ VIP Payroll	While employed at the school + 5 years
State Employees	Front Office	Engage/ VIP Payroll	While employed at the school + 5 years
Learnerships	Operations	Engage	While working for the school + 2 years
Temporary Staff	Finance/ Operations	Engage/VIP Payroll	While working for the school + 2 years
Learner Applications	Front Office	Engage/Physical Documents	2 years
Employment Applications	Front Office	MS Office/ Gmail/ Physical	2 years
Suppliers	Finance	Pastel	While supplying the school + 5 years
SGB	Front Office	Engage	While serving on SGB
Tenants	Operations	MS Office	While lease is active + 1 year
WCED	Front Office	MS Office	Indefinite
Past Learners	Operations	Engage/ Alumnet	Indefinite (via Rustenburg Alumnae)
Sponsors	Operations	MS Office	For period of sponsorship + 2 years
Advertisers	Operations	MS Office	For period of sponsorship + 2 years
Sporting Bodies	Sports Office	MS Office	Indefinite
SGB Associations	Front Office	MS Office	Indefinite
Unions	Front Office	MS Office	Indefinite
Statutory Bodies	Front Office	MS Office	Indefinite
Auditors	Finance	MS Office	While retained as service provider
Insurance Brokers	Finance	MS Office	While retained as service provider
Banks	Finance	MS Office	While retained as service provider
Attorneys/Debt Collectors	Finance	MS Office	While retained as service provider
Outsourced Service Providers	Finance	Pastel	While retained as service provider
Trustees	Finance	MS Office	While serving as trustees
Hostel Records	Erinville	MS Office	
Educational Inst.	Front Office	MS Office	Indefinite
Other School Records	Front Office/ Operations	MS Office	Indefinite

Appendix C:

The School:

Rustenburg Girls' High School
Campground Road
Rondebosch
7700

T: 021 686 4066
F: 021 686 7114
E: info@rghs.org.za

Principal:
Michael Gates
principal@rghs.org.za

Information Officer (IO):

Graeme Broster
Operations Manager
brosterg@rghs.org.za

Deputy Information Officer (DIO):

Francis Vogts
ICT Manager
vogtsf@rghs.org.za

Responsibilities of the IO/DIO:

The POPIA imposes the following responsibilities on an IO:

- Encourage and ensure POPIA compliance.
- Deal with POPIA related requests.
- Assist the Information Regulator with investigations when prior authorisation for processing activities were required and not obtained.

The POPI Regulations, impose the following additional responsibilities on an IO:

- Develop, implement, monitor and maintain a compliance framework.
- Ensure that a personal information impact assessment is done to ensure that adequate measures and standards exist to comply with the POPIA.
- Develop, monitor and maintain a manual in terms of the Promotion of Access to Information Act, 2000 (PAIA).

- Develop internal measures and systems to process requests for access to information.
- Ensure internal awareness sessions are conducted on the POPIA, its Regulations, codes of conduct and other information communicated by the Information Regulator.

The rising expectation of authorities that regulate the protection of privacy is that the organisation must be able to provide evidence not only that procedures are in place to protect personal information, but that they are actually being followed.

It is impossible to do so without assigning responsibility for the operational protection of personal information to an individual or individuals.

This individual may sit in a designated privacy function, or may be part of the Legal, Compliance, IT, Security or Information governance/management business units. Privacy may be the individual's full-time position (e.g., Privacy Officer) or may be one hat that the individual wears (e.g., Security Manager).

The privacy professional is responsible for:

- understanding the personal information collected, stored, used, shared, transferred and retired by the organisation
- facilitating strategy, policy, notices and operational procedures
- creating training programs
- managing security risk
- managing third party risk
- responding to inquiries and complaints
- overseeing a data breach program
- monitoring data practices
- reporting to internal and external stakeholders
- liaising with the Information Regulator
- formally demonstrating accountability

Steps to Assign Responsibility for the Protection of Personal Information

a) Establish the timeline for assigning privacy to an individual/s (DIO/Privacy Officer/Security Manager).
    - Is it immediate?

- Are there preliminary tasks that are to be done before such an individual is assigned?

b) Determine the responsibilities of the DIO/Privacy Officer/Security Manager:

- identify the regulatory requirements
- identify the relevant enterprise vision/values that relate to data privacy
- identify, if any, complementary duties

c) Discuss the approach for assigning the DIO/Privacy Officer/Security Manager:

- Will there be one DIO/Privacy Officer/Security Manager for the organisation?
- One per branch/business unit?
- A series of regional DIOs/Privacy Officers/Security Managers. (For example in the Provincial Departments of Health, Education and Social Development per region)?

d) Determine the reporting structure and create the enterprise organisational structure for the DIO/Privacy Officer/Security Manager.

e) Develop the job description(s).

f) Select the DIO/Privacy Officer/Security Manager:

- Interview the candidate(s).
- Make the selection.
- Obtain executive approval of the selection.
- Announce the selection and roles internally and inform those in the organisation of their supportive role of the DIO/Privacy Officer/Security Manager.

g) Register the IO (and DIO, where applicable) with the Information Regulator.[1]

[1] See section 55(2) of the POPIA.

Appendix D: Compliance Framework

The first Provincial Departmental POPIA Compliance Guide[2] was developed to assist and guide Provincial Departments towards compliance with the accountability condition, based on the Nymity Privacy Management Accountability Framework™. ("Accountability Framework"). The Accountability Framework is structured in thirteen privacy management processes ("PMPs") which make up an operational privacy framework and by adopting the Accountability Framework effect will be given to the obligation imposed by the POPI Regulations on the Information Officer to develop a compliance framework.

The purpose of this comprehensive guide is to assist organisations to implement and monitor compliance with the POPIA in accordance with the Accountability Framework. The first thirteen chapters are therefore aligned with the thirteen PMPs. Resources [3] are included at the end of each chapter as well as, where applicable, references to "Real World Samples" and some case studies. All templates may be modified according to each entities unique needs.

In addition chapter 14 includes guidelines and resources published by foreign authorities, akin to the Information Regulator, to assist organisations to take due regard of generally accepted information practices and procedures as required by POPIA.

A privacy management program should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The components should be regularly monitored, assessed and updated accordingly to keep pace with changes both within and outside the organisation. This may encompass changes in such areas as technology, business models, law and best practices.

– Privacy Management Programme, A Best Practice Guide
Office of the Privacy Commissioner for Personal Data, Hong Kong, Privacy Management Programme A Best Practice Guide, Hong Kong. *Management Program 2014, page 3.*

[2] POPI Act Compliance Guide Ver.1. 2015 Legal Services, Department of the Premier.
[3] Based on the Nymity Inc. Templates unless otherwise stated.

Accountability can be broken down into three elements, namely: (i) responsibility; (ii) ownership; and (iii) evidence.

Responsibility

Responsibility means that appropriate "privacy management activities" [4] have been implemented and are maintained on an ongoing basis.

Privacy management activities are ongoing procedures, policies, measures, mechanisms, and other initiatives that impact the processing of personal information or that relate to compliance with privacy and data protection laws.

No two organisations' privacy management is the same and thus appropriate activities are determined based on the organisation's compliance requirements, risk profile, business objectives, and the context of data processing (type of data processed, nature of processing, purpose for collection, use and disclosure, etc.).

Ownership

The ownership concept requires that an individual is answerable for the management and monitoring of each of the privacy management activities.

Even if the Information Officer is accountable for POPIA compliance, the Privacy Office (that part of the organisation tasked to ensure POPIA compliance) usually processes very little personal information, if any. As such, the effectiveness of privacy management relies on the appropriate privacy management activities being performed at all points of the personal information life cycle, from the point of collection to the point of destruction.

Ownership of some privacy management activities will reside within the operational and business units, for example, human resources (HR), marketing, product development, Information Technology (IT), customer service, etc., as that is where the personal information is being collected and processed.

Evidence

[4] To identify appropriate privacy management activities, Nymity's Privacy Management Accountability Framework™ is available at https://www.nymity.com/data-privacy-resources/privacy-management-framework.aspx .

The third element of a structured compliance framework is evidence. When privacy management activities are performed on an ongoing basis, evidence is produced as a by-product.

Evidence consists of documentation which may be formal (e.g., policies, procedures, reports) or informal (e.g., e-mail communications, meeting agendas, and system logs) and can be used with context by the Information Officer to show that a privacy management activity is being performed.

The table below outlines how formal and informal documentation can be produced, influenced, or collected by the Privacy Office as evidence of privacy management activities.

Privacy Management Activities	Evidence/ Documentation	Source/ Role	Formal/ Informal
Maintain a data privacy policy	Privacy Policy	Produced by the "Privacy Office"	Formal
Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts	E-mail Monitoring Policy and procedure	Influenced by the Privacy Office Produced by Information Technology (IT)	Formal
Provide notice in marketing communications (e.g. e-mails, flyers, offers)	Examples of e-mail marketing communications	Influenced by the Privacy Office and produced by Marketing	Informal
Provide notice in marketing communications (e.g. e-mails, flyers, offers)	Examples of e-mail marketing communications	Influenced by the Privacy Office and produced by Marketing	Informal

Privacy Management Activities are Ongoing

Privacy is not a project. Privacy management is a set of ongoing privacy management activities that are performed either periodically or continuously.

- **Periodic Activities** are performed on a set frequency, e.g. quarterly or annually. These activities are treated as discrete projects or tasks with a defined start and end.

- **Continuous Activities** are embedded into day-to-day operations. These activities often take a repetitive approach, wherein adjustments are made continuously toward the desired outcome.

The following table reviews privacy management activities to show how the two approaches for the frequency of activities might differ:

Privacy Management Activity	Periodic	Continuous
Maintain flow charts for data flows (e.g. between systems, between processes, between countries).	On an annual basis, require that key stakeholders review the flow charts for accuracy and update the diagrams as necessary.	Implement as part of the project management requirements that proposed changes to data flows are identified and the flow charts are updated as a condition of project sign-off.
Measure participation in data privacy training activities (e.g. numbers of participants, scoring).	Each quarter, review reports generated by the e-Learning system to determine whether all employees have completed the requirements.	Configure the e-Learning system to generate alerts when an employee has not completed the training by the required date and send a message to the employee's manager suggesting he or she follow up immediately.
Engage stakeholders throughout the organisation on data privacy matters (e.g., information security, marketing, etc.).	Establish a cross-functional committee of privacy stakeholders (e.g. IT, Marketing, Legal, HR, etc.) who meet on a quarterly basis to discuss data privacy matters.	Create an e-mail alias or group discussion for data privacy stakeholders, to facilitate communication on data privacy matters.
Maintain procedures to restrict access to personal information (e.g. role-based access, segregation of duties).	On a monthly basis, review reports of active system users to ensure their access is still appropriate and sign-off to indicate approval.	Configure the HR system to send alerts to Information Security when employees are terminated or when there are changes to the job title, department, or reporting structure.

Whether the activity should be performed periodically or continuously depends on a number of factors. Periodic activities may encourage structure, whereas continuous activities may provide more thorough coverage and risk prevention.

PRIVACY MANAGEMENT PROCESSES (PMPs)

1. **Maintain a Governance Structure**:
   Ensure that there are individuals responsible for privacy, accountable management, and management reporting procedures.
2. **Maintain a Personal Data Inventory**:
   Maintain an inventory of the location of key personal information storage or personal data flows with defined classes of personal information.
3. **Maintain a Privacy Policy:**
   Maintain a privacy policy to protect the personal information of data subjects that meets legal requirements and addresses operational risk.
4. **Embed Privacy into Operations**:
   Maintain operational policies and procedures consistent with the privacy policy, legal requirements, and operational risk management objectives.
5. **Maintain a Training and Awareness Program**:

Provide ongoing training and awareness to promote compliance with the privacy policy and to mitigate operational risks.

6. **Manage Information Security Risk:**
   Maintain an information security program based on legal requirements and ongoing risk assessments.

7. **Manage Third-Party Risk:**
   Maintain contracts and agreements with third parties consistent with the privacy policy, legal requirements, and operational risk tolerance.

8. **Maintain Notices**:
   Maintain notices to individuals consistent with the privacy policy, legal requirements, and operational risk tolerance.

9. **Maintain Procedures for Inquiries and Complaints:**
   Maintain effective procedures for interactions with individuals about their personal information.

10. **Monitor for New Operational Practices and Perform Privacy Impact Assessments**:
    Monitor organisational practices to identify new processes or material changes to existing processes, perform privacy impact assessments and ensure the implementation of Privacy by Design principles.

11. **Maintain a Privacy Breach Management Program**:
    Maintain an effective incident and breach management program to protect the personal information of data subjects.

12. **Monitor Data Handling Practices**:
    Verify that operational practices comply with the privacy policy and operational policies and procedures.

13. **Track External Criteria:**
    Track new compliance requirements, expectations, and best practices.