GUIDELINES ON THE PROTECTION OF PERSONAL INFORMATION ACT FOR DEPARTMENT OF BASIC EDUCATION

CHAPTER 1:

INTRODUCTION

The Protection of Personal Information Act (POPIA) aims to give effect to the constitutional right to privacy by balancing the right to privacy against that of access to information. POPIA requires that personal information pertaining to individuals be processed lawfully and in a reasonable manner that does not infringe on the right to privacy.

The constitutional right to privacy is contained in section 14 of the Constitution:
Section 14 of the Constitution provides that -
Everyone has the right to privacy, which includes the right not to have:

(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.

Section 2 of the Protection of Personal Information Act, 2013 (POPIA) sets out its purposes. The first purpose of POPIA is to:

(a) Give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at:

(i) Balancing the right to privacy against other rights, particularly the right of access to information, and
(ii) Protecting important interest, including the free flow of information within South Africa and across international borders.

POPIA gives content to the right to privacy as captured in the Constitution. It is not an absolute right and can be limited pursuant to the Limitations Clause in the Constitution. POPIA is an attempt to balance the right to privacy with the rights of others, including the right to access information.

POPIA's preamble recognises that:

(a) Section 14 of the Constitution provides that everyone has the right to privacy,
(b) The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information, and
(c) The state must respect, protect, promote and fulfil the rights in the Bill of Rights.

The enactment of POPIA is, in essence, the state's way of protecting, promoting and fulfilling the right to privacy as captured in the Bill of Rights.

THE LIMITATIONS CLAUSE

The right to privacy is not an absolute right. Constitutional rights may be limited, consistent with the Constitution. Section 36 of the Constitution (the Limitations Clause) captures the manner in which constitutional rights may be limited. All limitations of the right to privacy must be consistent with the Limitations Clause.

POPIA also recognises that the removal of unnecessary impediments to the free flow of information, including personal information, is required within the context of the constitutional values of democracy and openness, and the need for economic and social progress.

THE PURPOSE OF POPIA

As stated above, the first purpose of POPIA is to give effect to the constitutional

right to privacy. In doing so, it must be also deal with the limitations inherent with this right. The other purposes captured in POPIA are to:

a) Regulate the manner in which personal information may be processed;
b) Provide persons with rights and remedies to protect their personal information from processing that is not consistent with POPIA; and
c) Establish measures, including an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by POPIA.

THE APPLICATION OF POPIA

POPIA applies to the processing of personal information entered into a record by or for a responsible party. In order to understand the POPIA it is important that we familiarize ourselves with the following key terms as used in the POPIA:

Processing:

Processing is defined as 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;
(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.

Examples of processing would include; the personal information that the DBE requires relates and not limited to names and surnames, birth dates, identity numbers, passport numbers, demographic information, education information, occupation information, health information, addresses, union affiliation, memberships, and personal and work email and contact details.

Personal Information:

Means information relating to an identifiable, living, natural person, and where it is applicable to, 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;
(d) the biometric information of the person;
(e) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature;

Examples of personal information would include someone's home, postal and email addresses, fingerprints, views expressed in an evaluation form at a workshop and their information captured in a curriculum vitae.

Record:

Means any recorded information:

(a) Regardless of 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) Label, marking, or other writing that identifies or describes anything or which it forms part, or to which it is attached by any means;

(iv) Book, map, plan, graph or drawing;

(v) 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 the responsible party; and

(d) Regardless of when it came into existence.

Examples of personal information would include taking pictures of someone, writing down and storing their details, scribbling down a person's identity number on a piece of paper.

The responsible party must in essence be domiciled in South Africa or, if not domiciled in South Africa, making use of a means of recording in South Africa –

unless those means are only used to forward personal information through South Africa.

Summary of key points

- POPIA gives effect to the constitutional right to privacy.
- The right to privacy is recognised as an independent personality right.
- POPIA applies to the processing of personal information entered into a record by or for a responsible party.
- POPIA is aimed at safeguarding personal information when processed.
- The right to privacy is subject to justifiable limitations.
- POPIA captures rights and remedies to protect personal information.

CHAPTER 2:

RELEVANCE OF THE POPIA TO DBE

The POPIA is relevant to DBE as personal information is ordinarily processed as part of the nature of the services offered. POPIA imposes a number of obligations when processing personal information.

POPIA is a law of general application that applies to the processing of personal information and defines a person as a natural or juristic person.

The following are some examples of when the DBE as the responsible party processes personal information:

(a) Employment Contracts Employees
(b) Service Provision Consultants, Service-Providers,
(c) Experts
(d) Recruitment Job applicants
(e) Information Dissemination including website participants
(f) Customer Relations Complainants
(g) Emergency Contacts Relatives of certain data subjects
(h) Legal Services Clients
(i) A data subject is the person to whom the personal information relates.

Personal Information: means information relating to an identifiable, living, natural person, and where it is applicable to, an identifiable, existing juristic person. The data the DBE has access to is extensive. Much of it is ‘personal information’ in terms of POPI Act. In particular, the 13-digit national identity number of learners and employees, as well as their names, gender, and date of birth can be found in the data. The provincial education departments need the personal information for operational purposes, and as the source of much of the DBE’s data is the provincial departments, personal information is included.

In terms of the National Education Policy Act (NEPA), the use of data by the DBE is limited to monitor and evaluate progress to comply with the Constitution and the national education policy. Data may either the gathered from EMIS or other suitable means, in co-operation with provincial departments of education. The use of educators' cell phone numbers must be limited.

Importantly, for analytical purposes and for the fulfilment of NEPA monitoring obligations, the personal data the DBE has is required. In particular, personal information is needed when different data sources must be linked. For example, if an analysis must be conducted of how well Grade 12 examination candidates performed in grades below Grade 12, then the Grade 12 examinations data must be linked to separate datasets covering lower grades.

It is often necessary to use multiple variables in linking data sources because one variable on its own will display limitations. For instance, the 13-digit identity number links most learners across the Grade 12 examinations and pre-Grade 12 datasets, but not all, as some identity numbers are missing. In this instance, the use of names and dates of birth can be used to fill the gap, but also to verify the accuracy of national identity number. Importantly, the monitoring work referred hereto never involves the revelation of personal information in the DBE reports which are produced as part of the process. The reports will only reflect statistics at an aggregate level relating to, for instance, drop-out rates.

The National Education Policy Act (Act 27 of 1996), referred to below as NEPA, requires the DBE to conduct planning, research and monitoring for the Minister of Basic Education for the furtherance of national goals. In doing this, the DBE produces many internal and public reports each year that are based on the data it has access to, in a wide range of areas that include school attendance, the opening and closing of schools, the employment of teachers, and learner performance. In terms of NEPA, the DBE is also required to advance the use of data in the broader 'national education system',

which includes promoting data use across various government entities where this generates knowledge which is important for the education sector.

The DBE is routinely involved in exercises where DBE data is linked to other government data for the purposes of verifying data quality, and of monitoring. For instance, the DBE and the South African Social Security Agency (SASSA) collaborate, using a variety of personal information fields, to determine if social grant recipients who are of school-going age are attending school. Linking, in collaboration with the Department of Higher Education (DHET), the records of learners previously enrolled in schools to those of students currently in post-school institutions is important for understanding flows between the two education levels. Section 57(1)(a) of the POPIA indicates that, prior authorisation must be obtained from the Information Regulator before a unique identifier (such as an ID number) is used for a purpose other than the one for which it was intended at the time of collection, with the purpose to link the information with information processes by other responsible parties.

Summary of key points

(a) Attorneys ordinarily process personal information.

(b) Attorneys must, before entering into a client relationship, establish and verify the identity of prospective clients to engage in a business relationship or to conclude a single transaction

CHAPTER 3:

HOW TO PROCESS INFORMATION LAWFULLY

POPIA introduces specific legal responsibilities for managing and processing personal information under its control. Compliance with POPIA will:

(a) Ensure the protection of the personal information within the possession of DBE;
(b) Increase stakeholder confidence and relations;
(c) Minimise exposure to unnecessary risks; and
(d) Help to protect the sectors reputation.

Non-compliance with POPIA, on the other hand, may lead to:

(a) Exposure to unnecessary financial and reputational risks;
(b) Adverse media publicity;
(c) Negative public perceptions;
(d) Fines issued by the Information Regulator; and
(e) Civil action by the data subject.

It is absolutely vital that all information provided is handled correctly. The rights of data subjects are defined in POPIA. Data subject is the person to whom personal information relates.

Section 5 of POPIA captures the following rights, amongst others, of data subjects:

(a) To be notified of the collection of their personal information,
(b) To be notified that their personal information has been accessed or acquired by an unauthorised person,
(c) To establish what personal information is held by DBE,
(d) To request access to their personal information,
(e) To request the correction, destruction or deletion of their personal information,
(f) To object, on reasonable grounds, to the processing of their personal information,
(g) To object against the processing of their personal information for purposes of direct marketing (including solicitation of funding) through unsolicited electronic communication.

As indicated in Chapter 2, processing includes the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of personal information and dissemination thereof by means of transmission, distribution or making available in any other form.

The processing of information must be done in accordance with the provisions of POPIA to be considered lawful. Section 4 of POPIA lists the eight conditions for lawful processing of personal information, which are:

Accountability

The DBE must appoint a party (Information Officer) who will be responsible for ensuring that the information protection principles within **POPI Act** and the controls that are in place to enforce them are complied with.

To aaccept responsibility is to comply with the responsibilities under POPIA;

(a) Approve suitable policies and systems for the management and processing of personal information;
(b) Ensure that policies and systems are understood, embraced and complied with;
(c) Ensure that staff members are properly equipped and trained to comply with POPIA;
(d) Ensure that contracts with employees third parties capture relevant POPIA responsibilities; and
(e) Regularly monitor and review the effectiveness of policies and systems.

Processing Limitation

The DBE must ensure that there is lawfulness of processing, minimality of information collected, consent, justification and objection, and the collection of personal information directly from the data subject.

Section 9 requires that the processing of personal information be conducted lawfully and in a reasonable manner that does not infringe the data subject's privacy. In essence, there must be a legal basis for the processing of personal information of any data subject. The clearest way perhaps is to establish such a lawful basis, is through the consent of the data subject.

The **PURPOSE FOR PROCESSING** personal information must be:

(a) Adequate
(b) Relevant
(c) Not Excessive

When is the processing of personal information lawful?

Personal information may only be processed (including, collected, received, recorded, organised, collated, stored, updated, altered, disseminated) if:

(a) The data subject consents to it;
(b) A competent person (parent or guardian) where the data subject is a child, consents to it;
(c) It is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;
(d) It complies with an obligation imposed by law on the responsible party;
(e) It protects a legitimate interest of the data subject; or
(f) It is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Can a data subject withdraw consent to and object to processing?

- Yes, a data subject (or a parent or guardian of a child) may at any time withdraw his or her consent in situations where consent was given.

A data subject may, unless the law allows for such processing, object on reasonable grounds to the processing of personal information by the DBE in situations where the processing:

(a) Protects a legitimate interest of the data subject, or
(b) Is it necessary to pursue the legitimate interests of the attorney or a third party to whom the information is supplied?

This objection must be done in the prescribed manner.

A data subject may also object to the processing of personal information for purposes of direct marketing (including solicitation of funding).

Withdrawal of consent and objection against the processing

POPIA requires that the processing of personal information of a data subject be stopped where the data subject objected thereto. POPIA does not specifically explain what will happen in the event that there is a dispute between the parties as to the grounds on which the objection is based.

Purpose Specification

The personal information must be collected for a specific purpose and the data subject from whom the personal information is collected must be made aware of the purpose for which the personal information was collected. POPIA requires that PURPOSE FOR COLLECTING personal information must be:

(a) Specific
(b) Explicitly Defined
(c) For a Lawful Purpose related to the function or activity of the attorney

Personal information must not keep for longer than necessary for achieving the purpose for which it was collected or processed unless:

(a) The law requires such a retention period,
(b) The DBE requires such a record for lawful purposes,
(c) Retention is based upon a contract between the parties,
(d) The data subject has consented to such retention, or
(e) A competent person on behalf of a minor has consented to such retention.

Personal information may be retained for historical, statistical or research purposes for longer periods provided that appropriate safeguards is established for the records being used for other purposes.

Personal information once they are no longer authorised to retained must be destroyed, deleted, or de-identified.

De-identifying means to delete information that—

(a) Identifies the data subject;
(b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

Further processing Limitation

If a responsible party further processes personal information, such processing must be compatible with the purpose for which the information was collected. POPIA requires that further processing of personal information must be consistent with the purpose for which it has been collected. In essence, the information collected for one purpose should not be processed and used for another process.

To assess the compatibility between the purpose for collection and the purpose for processing, the following factors must be taken into account:

(a) The relationship between the purpose for the collection and the purpose for further processing;
(b) The nature of the information concerned;
(c) The consequences for the data subject of the further processing;
(d) The manner in which the personal information has been collected; and
(e) Contractual rights and obligations between the parties.

Further processing of personal information is permissible in certain instances, including, where:

(a) The data subject has provided consent;
(b) The personal information is available on a public record; or
(c) The data subject has deliberately made public such personal information.

Information Quality

The responsible party must take reasonable steps to ensure that the personal information that has been collected is complete, accurate, not misleading and up to date. In so doing, the responsible party must take into consideration the purpose for which the personal information was collected.

Openness

The responsible party must be open about the collection of personal information by notifying the Regulator if it is going to process personal information and, if personal information is going to be collected, the responsible party must take "reasonably practicable steps to ensure that the data subject has been made aware that his or her personal information is going to be collected. The responsible party should for example, take reasonable steps to make the data subject aware of its name and address, and the purpose for which the personal information being collected.

Non-compliance to the above permitted in the following situations:

(a) The data subject has consented to non-compliance
(b) Non-compliance is necessary to comply with a legal obligation
(c) Non-compliance is necessary for the conduct of court proceedings
(d) Non-compliance is necessary in the interests of national security
(e) Compliance would prejudice a lawful purpose of the collection
(f) Compliance is not reasonably practicable in the circumstances
(g) The information will not be used in a way to identify the data subject
(h) The information will be used for historical, statistical or research purpose.

Security Safeguard

The responsible party must ensure that the integrity of the personal information in its control is secured through technical and organisational measures in order to prevent:

(a) Loss of, damage to or unauthorised destruction of personal information; and
(b) Unlawful access to or processing of personal information.

The responsible party must:

(a) Identify all reasonably foreseeable risks to personal information;
(b) Establish and maintain appropriate safeguards against risks;
(c) Regularly verify that safeguards are effectively implemented; and
(d) Ensure that safeguards are continually updated.

Data Subject Participation

The data subjects have the right to request that a responsible party confirm (free of charge) whether it holds personal information about the data subject, and he or she may also request a description of such information.

In terms of section 10 of the POPI Act, personal information may only be processed if certain conditions, listed below, are met:

a) The data subjects or a competent person where the data subject is a child, consents to the processing; or
b) The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
c) Processing complies with an obligation imposed by law on the responsible party; or
d) Processing protects a legitimate interest of the data subject; or
e) Processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom information is supplied.

Summary of key points:

Section 4 of POPIA lists the following eight conditions for lawful processing of information as illustrated above.

CHAPTER 4:

SAFEGUARDING PERSONAL INFORMATION

The DBE has secured the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of or damage to or unauthorised destruction, unlawful access to or processing of personal information.

The DBE employs stringent data security protocols, in line with government-wide rules, when it comes to the storage of original datasets. Data analysis required to comply with NEPA necessarily involves analysts working with the data on their computers, on which statistical analysis software has been loaded. Such work could be focussed on monitoring, research, scenario-building or data quality verification.

In advancing the goals of NEPA, it may be necessary for analysts in government entities outside the DBE to work with the data containing personal information. To reduce the risk of theft or some other unauthorised sharing of personal information, two things are necessary. Firstly, the time during which personal information remains on a personal computer should be minimised. Secondly the management of the personal computer in question while personal information is stored, should be sufficiently secure.

The POPIA requires that personal information in their possession be safe-guarded. Processing includes automated and non-automated means. DBE should take appropriate measures to prevent:

(a) Loss of, damage to or unauthorised destruction of personal information, and
(b) Unlawful access to or processing of personal information.

Personal information may get lost, damaged or unlawfully accessed in a variety of ways, including:

(a) Theft of documents or electronic records,
(b) Computer viruses,
(c) Computer crashes,
(d) Hacking of databases,
(e) Accidental damage caused by employees or contractors, or
(f) Natural disasters.

An effective IT security system involves safeguarding the computer hardware and the personal information stored on the hardware.

The following steps are listed in POPIA:

Identify all reasonably foreseeable risks to personal information. A risk assessment on personal information would be valuable, and the LSSA proposes that attorneys implement it. The risk assessment should basically cover the following-

- Identify the nature of the personal information in the DBE's possession,
- Identify key risks involved with the collection, storing and processing of personal information, and
- The implications for the data subjects should their personal information get lost, unlawfully accessed or destroyed.

Once it is clear on the risks involved with personal information, he or she should decide on appropriate safeguards.

Summary of key points:

(a) An effective IT security system involves safeguarding the computer hardware and the personal information stored on the hardware.

(b) Cloud computing takes various forms and will in most cases, inevitably result in the processing of personal information of data subjects.

ANNEXURE A: POPIA CHECKLIST

A. APPOINT AN INFORMATION OFFICER

(1) It is advisable to appoint the same Information Officer for both PAIA and POPIA.
(2) Appoint the same Deputy Information Officer for both PAIA and POPIA.
(3) Formally agree the Information Officer and Deputy Information Officer's roles and responsibilities, including reporting structures and mandatory reporting regularly [maximum timeframe should be monthly)
(4) Complete the formal appointment process by issuing a letter of appointment with role and responsibility.

B. PROCESS

(1) The process followed should be a similar process followed by a basic Risk Management process.
(2) Risk and Opportunities must be considered, and cost-effectiveness should be the guide.
(3) Various scenarios with multiple mitigation actions must be developed
(4) Mitigation in this instance will be the action that ensures compliance to key risks identified.

C. GAP ANALYSIS

(1) Ensure key internal stakeholders are part of this process or a cross-section of staff from different sections
(2) Assess and review existing process and risks against POPIA
(3) Set interim and final targets for compliance with the POPI Act.
(4) Use an evidence-based approach

D.ANALYSIS OF THE PROCESSING AND STORAGE OF PERSONAL INFORMATION

(1) This section is the critical part of the Policy.
(2) Utilise the POPIA definitions and record types.
(3) POPIA requires at the minimum6: consent, purpose, source, sharing, destruction.
(4) Capture only necessary information.
(5) Ensure the right to access and capture information is necessary [refer to POPIA, which details the rights to access and the link to business information required].
(6) Consider user rights and the management thereof in terms of the ICT Policy
(7) Digital data storage must be considered in terms of access [passwords], limitation of users [access] and password policy [mandatory expiry requiring change, defined structure – minimum length, special characters] etc.
(8) Paper-based information must be securely stored and when information is not needed [subject to SARS, Financial Intelligence-FICA requirements etc.]

E. IMPLEMENT POPIA COMPLIANCE POLICIES

(1) Review all current policies that POPIA impacts.
(2) Ensure the policies and procedures are appropriate and adequate.
(3) Policies are only of use if they are monitored and enforced. Failure is negligence on the part of management.
(4) Ensure the Policy is distributed and included in all policy manuals for all staff.
(5) Using a rational method for reaching reliable and reproducible conclusions in a defined and systematic process. The approach outcomes or estimate must be relevant, sufficient and verifiable.
(6) These must be detailed as per the requirements of POPIA
(7) Ensure the Policy is explained to all staff and fully understood with staff signing that they have understood the objectives and the processes to confirm when and how data is captured and stored.

(8) The framework must be discussed with staff at least quarterly to ensure the safeguards and risk mitigation is still applicable and relevant.
(9) Stakeholder groups must receive an appropriate notification that is specifically designed for various target groups.
(10) Third-party risks must be specifically managed.

F. WEBSITES AND OTHER SECURED WEB AND ONLINE STORAGE SITES

(1) Establish a process for reviewing websites.
(2) Ensure disclaimers are adequate.
(3) Ensure no personal information is outward-facing [i.e. visible to users].
(4) Ensure cache information and personal information is protected against malware, cyber and other digital intrusions.
(5) Develop a schematic approach to red flag high risk and priority info.
(6) Ensure benchmark standards ICT are employed and get formal assurance from hosting providers and other website services used.
(7) All risk mitigation requires a crisis plan, ensure this is developed for POPIA – these are generally standard and encompasses a communication plan should there be a breach.

G. POPIA MANUAL

(1) Ensure your POPIA manual is ready and staff trained by 1 July 2021
(2) If already in place, review your POPIA manual
(3) Ensure your manual follows the prescribed format as per the POPIA and minimum standards.
(4) This refers to outsourced suppliers and service providers which encompasses unique risks as they have access to personal information and in many instance has access to digital files and information. Outsourced paper storage requires its own risk mitigation

I. TRAINING IN POPIA COMPLIANCE

(1) Training is tailored to the needs and requirements
(2) Training like other risk training [cyber, ICT etc.] must be continuous and adapt to the changing environment and the evolution of risks.
(3) Online, and hybrid training is the norm, and there can be no excuse for lack of training.
(4) Business excellence Model sample slide is attached for engagement with all staff who are involved with data and personal information.
(5) Results or statistics that are abnormal compared to the majority of results [standard]

J. POPIA COMPLIANCE IS INTEGRATED INTO THE BUSINESS PROCESS

(1) POPIA must be treated as other risk management in the DBE and must be integrated into all relevant business processes.
(2) The processes and systems must be seamlessly integrated into all business process.
(3) Like all risk management, it requires vigilance and review to ensure trends, regulations; legislation is reviewed for both risks and opportunities.
(4) Risk management must be reviewed on how it impacts the practice achieving its objectives, both negatively and positively.
(5) The potential negative impact may require mitigation, and opportunities can be grasped. However, ultimately these are all business decisions.