POPIA ACT: Overview and Application (in effect from 1 July 2021)

1. Definition

POPIA stands for the Protection of Personal Information Act.

2. Legislative Content

POPIA does the following:

2.1. Introduces minimum safeguards for protection of personal information; regulate the manner such information is processed.

2.2. Provides rights, remedies to protect personal information. Overlap with other laws – ensure the highest privacy standard prevails.

2.3. Establishes an Information Regulator – appointed in 2016.

2.4. Applies to all organisations and individuals, with some exceptions or exemptions as may be granted by the Regulator.

2.5. Regulations published in December 2018 (deals mostly with investigations and duties of Information Officers).

2.6. Effective from 1 July 2020 – 12-month grace period - must be in place by 1 July 2021

3. Terminology

3.1. *Data Subject* - to whom the personal information belongs

3.2. *Responsible person* - the person/entity who determines the purpose and means for processing personal information in their possession (Information Officer);

3.3. *Operator* - the person (or third party) doing the actual processing;

3.4. *Information Regulator;*

3.5. *Personal information* - Information relating to an identifiable, living natural person; or an identifiable, existing juristic person, including:

3.5.1. 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

3.5.2. Education, medical, financial, criminal or employment history

3.5.3. Any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment (would include online identifiers);

3.5.4. Blood type or other biometric information;

3.5.5. Personal opinions, views or preferences;

3.5.6. Private correspondence or further correspondence that would reveal contents of the original correspondence;

3.5.7. The views or opinions of another individual about the person; and

3.5.8. Name of a 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;

3.5.9. *Special categories of personal information - (stricter processing obligations)*

3.5.9.1. Religious or philosophical beliefs;

3.5.9.2. race or ethnic origin;

3.5.9.3. trade union membership;

3.5.9.4. political persuasion;

3.5.9.5. health or sex life;

3.5.9.6. Biometric information;

3.5.9.7. criminal behaviour of a person (E.g. medical records, pre-employment verifications, drug test results)

4. Obligations of Grace Primary School (Information Officer - see Annexure C)

4.1. secure the integrity and confidentiality of the personal information;

4.2. take appropriate, reasonable technical and organisational measures to prevent the loss of, or damage to the personal information;

4.3. Prevent unlawful access to, and unauthorised processing or destruction of the personal information;

4.4. identify internal and external risks to the personal information;

4.5. establish and maintain appropriate safeguards against losing or damaging personal information;

4.6. regularly verify the safeguards; and ensure that the safeguards are continually updated.

5. Information Processing Principles

5.1. Accountability: *Duties of Information Officer*

5.1.1. Gather information about use of personal data in all areas of the school

5.1.2. Do gap analysis to determine level of compliance – conduct preliminary assessments

5.1.3. Investigate, define and compile a plan to establish an Information Security Management System,

5.1.4. A compliance framework (and remedial action) to be developed, implemented and monitored.

5.1.5. Encourage and ensure compliance with POPIA - internal policies and procedures

5.1.6. Awareness sessions in the organisation

5.1.7. Implementation and monitoring; maintenance of adequate processing measures

5.1.8. Requests for access to information (internal and external)

5.1.9. Liaison with Regulator; investigations

5.1.10. Develop Incident Response Plan

5.2. Processing limitation

5.2.1. Personal information should only be processed in a limited and lawful manner that does not unnecessarily infringe the privacy of the data subject (Example: Employee-data – lifecycle of employment);

5.2.2. The processing must be adequate, relevant, not excessive; and only where certain specified circumstances exist (only 6 grounds):

5.2.2.1. When consent is given (consent may under certain circumstances be withdrawn);

5.2.2.2. When processing is necessary to carry out a contract to which the data subject is a party;

5.2.2.3. When the processing complies with an obligation imposed by law;

5.2.2.4. Where processing protects a legitimate interest of the data subject;

5.2.2.5. When processing is necessary for the performance of a public duty by a public body; or

5.2.2.6. In pursuit of the legitimate interest of the responsible party or of a third party to whom the information is applied.

5.3. Purpose specification:

The purpose for which personal information is collected, must be specific, explicitly defined and lawful.

5.4. Further processing limitation

Further processing must be compatible with the purpose for which the personal information had been collected.

5.5. Information quality

Take reasonably practicable steps to ensure personal information is complete, accurate, updated and not misleading.

5.6. Openness

Data subject must be advised of certain mandatory information regarding collection of personal information.

5.7. Security safeguards

Integrity and confidentiality of the personal information must be secured

6. Data breach – mandatory notification by the School

If there are reasonable grounds to believe personal information has been accessed / compromised / acquired by unauthorised party – notification must be given to:

6.1. The data subject (if identifiable);

6.2. The Regulator

6.2.1. As soon as possible after discovery

6.2.2. Notification to data subject in writing

6.2.3. Sufficient information for data subject to take protective measures

6.2.4. Regulator may direct publication of data breach

6.2.5. Importance of an Incident Response Plan (PR, legal, IT, HR, management)

6.2.6. Legal liability / criminal offence

7. Data Subject Participation

The data subject has certain rights of access to their personal information, such as correction or deletion.