DATA MANAGEMENT POLICY
(POPI ACT POLICY)
LORETO CONVENT SCHOOL
REVISED MARCH 2021

Policy Title
Data Management Policy (including the Protection of Personal Information Act, 2013)

Preamble

Data Management forms a vital part of the effective management and daily functioning of any school. In order to operate legally and efficiently, there is an amount of information that is required to be kept and accessed for every learner and staff member, as well as a time period that that information would need to be kept to comply with legislative requirements.

The primary objective of data management is to prevent the loss of data and associated information, to ensure timely, efficient and open access to the best possible data, and associated information, for use and re-use throughout its life-cycle. There are too many instances where valuable data sets have been lost through accident or neglect, or not been accessible as they are stored in non-digital form or on staff member's own workstations.

Moreover, in view of the considerable investment required to collect and store data, it is critical that it is managed in a way that maximises its utility and impact and thus its benefit to the larger school community.

In order to do this, accurate records, as well as the necessary documentation, needs to be kept, utilised correctly and stored effectively.

Purpose

The Learner Data Management Policy will give guidelines as to what data will be gathered, how it will be stored and correctly utilised. This policy also makes accommodation for the POPI Act, coming into effect on 1 July 2021.

Scope
This Data Management Policy will apply to parents and learners from Grade RRR to Grade 12 at Loreto Convent School, as well as all members of staff employed by the School.

Policy Guidelines

School records are documented evidence of what a school does. School records contain data and information about various aspects of a school's operations, including data about its students,

teachers, classes, facilities and finances. The main purpose of a SRMS (School Records Management System) is to systematically record, store and update the school's records.

The information from the SRMS is used to support evidence-based management of the school. School managers regularly make decisions about their school's operations. To make good decisions, school managers need information that is up-to-date and accurate. A SRMS helps school managers to systematically collect, store and analyse information about their school so they have relevant and reliable information readily available to support decisions they make in running the school.

People who are responsible for making education policy – and for planning and managing the education system – realize that both the quantity and quality of data needed to support evidence-based decisions improve when schools systematically maintain and use school records.

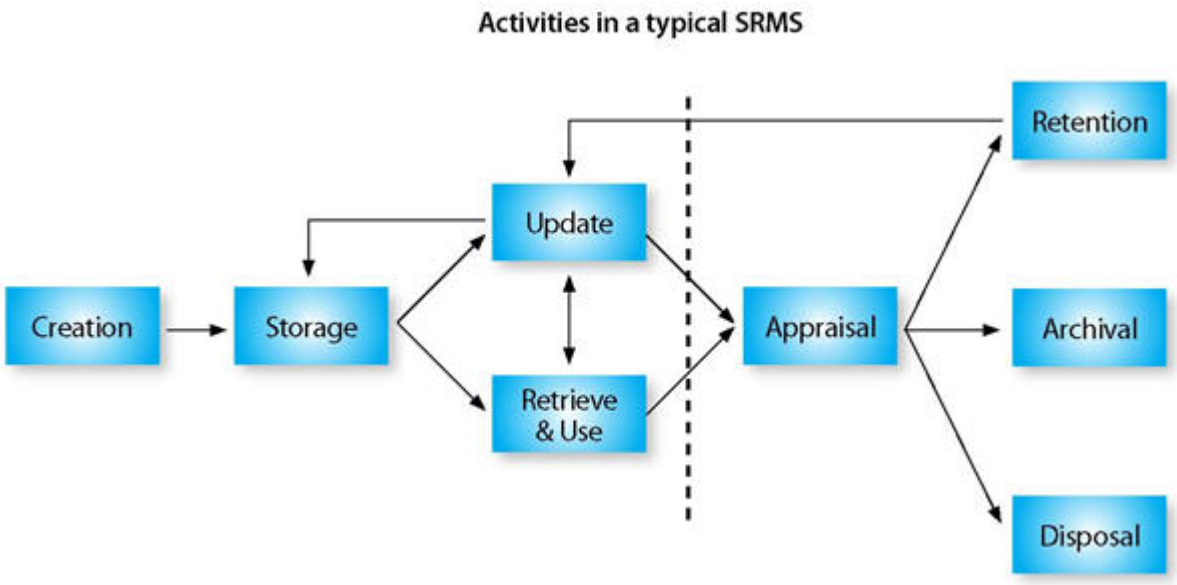
Furthermore, improving data and information management in schools is crucial to decentralized management and accountability in the education system. The implementation of a SRMS can help to distribute accountability throughout the school system, and enable the schools to better inform and cooperate with their local communities.

Complying with the enactment of the POPI Act is critical in ensuring that the correct procedures are followed to protect data gathered and disseminated by Loreto Convent School and will ensure that the school meets its statutory requirements.

The School Records Management Process

A School Records Management System typically involves the following eight activities (see Figure below):

1. **Creation** – beginning a new record and starting to record data and information, for example creating a student record card for a new student.
2. **Storage** – keeping the records in an organized manner so they can be accessed by authorized people but kept secure from unauthorized access, loss or damage.
3. **Update** – adding new information to a record or modifying existing information in a record.
4. **Retrieval** – searching for, locating and extracting records from storage.
5. **Use** – applying information from the records to help make management and policy decisions.
6. **Appraisal and Retention**– determining whether and how long a record should be:
    - retained for active use;
    - archived; or
    - disposed of.
7. **Archiving** – storing inactive records so they can be later retrieved for use.
8. **Disposal** – discarding, deleting or destroying a record.



In a school such as Loreto Convent School, the SRMS has to involve various school staff to systematically record data and information about different aspects of the school's operations. We use specific, pre-designed school record forms and follow procedures that are defined by school regulations and requirements. Different staff are responsible for different school records and procedures in recording, storing, updating and retrieving information. At the end of each school year, the records that have been accumulated are appraised to determine which records should be retained, archived or disposed of.

A good SRMS is characterized by organized classification and filing of the school records in a way that makes it easy to search, access, retrieve and use the recorded data and information. Records about the same topic or issue are grouped and arranged in a logical order, such as by alphabetical order, chronological order, or sorted by other criteria. For example, individual student records can be classified and filed by grade, class or subject. Teacher records can be sorted according to years of service, and school facilities by type of facilities, etc.

If the information is recorded on paper, each file will group together all relevant supporting documents such as detailed inventories, receipts, invoices, payment records, copies of important correspondence and other related documents. If the records are computerized, such paper evidences can be scanned and stored in electronic format.

The Data Management System utilised at Loreto Convent School, can help to manage school records by storing information in a way that allows for rapid sorting, searching and retrieval of data. Besides reducing the use and handling of papers, an additional advantage of our computerized system is that it can help to analyse the recorded data and quickly generate various summary statistics, performance indicators, tables and graphs, and even detailed school management information such as lists of students and teachers who were absent on a specific day, or misdemeanours kept on record for detentions.

Each of the record management functions (items 1 to 8 above) has a direct influence on the availability of information and their use for school management. Since various people in a school generate and use information, poor recording of key school management information and poorly managed school records can seriously affect the efficiency and effectiveness of a school. To

systematically manage school records, each person must assume their respective roles in creating and updating school records using correct records forms, terminology and practices, and submit the record files to the designated place of storage on time (see Section 4 for further details).

Record management is also vital in providing the Department for Basic Education with statistics, and required information on a monthly and annual basis. (eg. Absentee reporting, Valistractor uploads, database deployment to the Head Office, SA-SAMS and other information, as required by the DBE.)

What Does the SRMS Record?

Based on a review of school management practices in many countries, school records should give priority to recording data and information about the following aspects of school:

1. **Students** – personal and family information, previous educational experience, current grade, attendance, academic performance, behaviour, achievements/faults, outcomes (e.g. promotion to next grade, repeating grade, drop-out, transfer, or graduation).
2. **Teachers** – personal characteristics, past education, qualification, pre-service and in-service teacher training received, years of service, employment status, subject specialization, class/subject taught, teaching load, special skills, attendance, performance, behaviour, achievements/faults.
3. **Finance** – school budget and income by source, expenditure by type, financial balance and all other information pertaining to the daily accounting function of the bursor.
4. **Physical Facilities** – quantity and conditions of school buildings, classrooms, furniture, equipment and other physical facilities; maintenance, repairs and new constructions; rate of utilisation.
5. **Teaching/Learning Materials** – quantity and conditions by type of material, new acquisitions, rate of utilisation.
6. **Learning Achievement and Outcomes** – results of tests, examinations and assessments (regarding academic, behavioural and other student attributes).
7. **Extra-Curricular and Co-Curricular Activities** – type of activities, schedules, staff involved, number of participants, results, impact.
8. **School and Community Interactions** – school governing board meetings, parent-teacher association activities, school-and-community activities.
9. **Gauteng Department of Education** – all correspondence with the school, surveys and requested information, absentees and registers, exam registration for Grade 12 NSC exams

Based on good practices in school management and the need to monitor progress toward EFA goals, the following records are essential for SRMS in Loreto Convent School:

1. Application Information and Registration Forms
2. Learner Profile
3. Class Registers
4. Learner performance summary (Report Card)
5. Teacher CV, ID and other Relevant Information in a Personnel File
6. Teacher performance evaluation report (Annual Survey)
7. Inventory of physical facilities
8. Inventory of furniture/equipment
9. Inventory of teaching/learning resource materials

10. Financial Records with Applicable Reports
11. Department and physical Post Register

These eleven essential school records, when systematically kept, updated and used by the schools, will not only strengthen information management within our education system, but also enable each school, district, province and central education authorities to effectively monitor many aspects of the School's Administration.

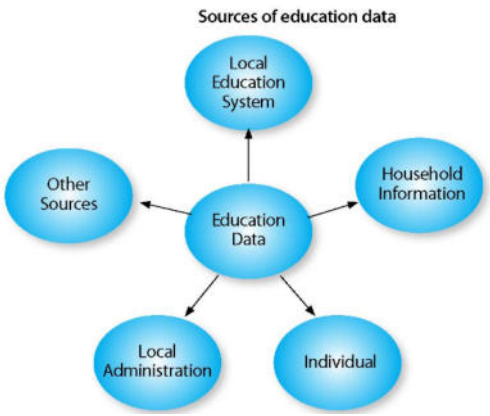
For school managers, administrative staff and teachers to better plan, organize, conduct, monitor and evaluate their daily school activities, additional school records may be created and used such as detailed financial ledgers, records of presence of school staff, records of use of school facilities and teaching-learning materials, school meals and scholarships, etc. Separate school records can be created and updated about extra-curricular and co-curricular activities organized, finance committee meetings, school management board meetings, other school-and-community activities, after each such activity has taken place. Those additional records that are found to be most useful can become regular components of the school's SRMS.

To help school staff to correctly perform their SRMS tasks, initial training should be organized, either by the school Principal or a knowledgeable member of SMT. This training should include general school records management principles, terminology and practices, as well as training about how to manage specific school records. Try to ensure that at least two staff in each school know how to maintain each type of essential school record, so there will be no interruption even if one of the two staff is absent. If necessary, such training can be supported by the selected third party application establishments. (Principal Primary, Pastel, SA-SAMS etc)

Once the school staff are trained in school records management, the school principal and experienced staff and SMT, should continue to provide regular advice, supervision and support to ensure that all staff apply what they have learnt to properly create, update, store and use school records in a correct and timely manner.

DATA COLLECTION

Data can be collected from the following sources:



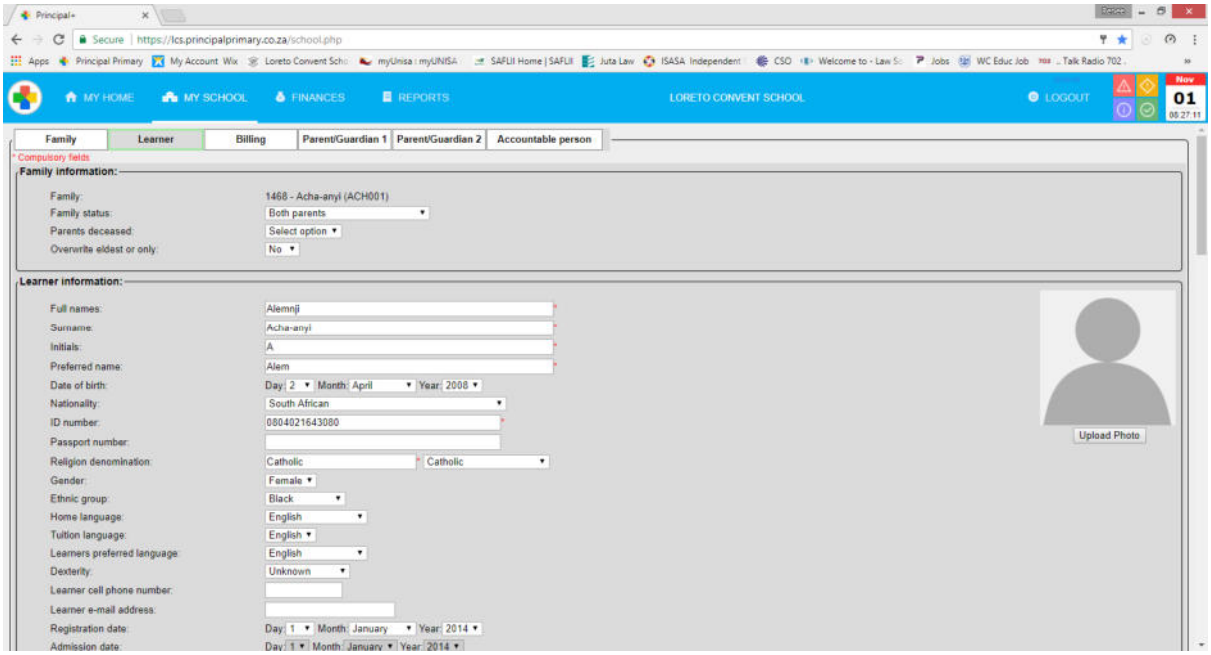
LEARNER DATA:

1. Upon the application of any prospective learner, the following information is requested by the school, to open an admissions file:

    - TWO copies of the learner's birth certificate
    - TWO recent ID Photos of the learner
    - The learner's baptism certificate (if available)
    - The learner's most recent School Report
    - Proof of residence
    - Proof of income (both parents)
    - Financial clearance notice from current school (or latest statement)
    - If self-employed, 3 months' bank statements
    - If not a South African Citizen:
        - Passport of parents and learner
        - Valid Student Visa/Study/Residence Permit for parents and learner
        - 3 Months' Bank Statements

2. Once the prospective learner is accepted into the school, a Registration Form is completed by the parent, which further gathers information required by the Data Management System (PRINCIPAL PRIMARY).
3. Every learner is issued with a Learner Profile. Should the learner come to Loreto from another school, the profile is requested from the school. All print information is stored in the Profile.
4. Data is captured to the PRINCIPAL PRIMARY system once a learner is registered and accepted.
5. Once the learner commences their education at Loreto Convent School, data can be added to the system as and when required.
6. Report Cards and any other relevant information (warning letters, prizes and awards, etc) are added to the Learner Profile.
7. When a learner transfers to another school, the profile is sent to the relevant school.
8. When Grade 12 learners finish their schooling at Loreto Convent School, their profiles are securely stored for a period of 5 years, where after they are destroyed.

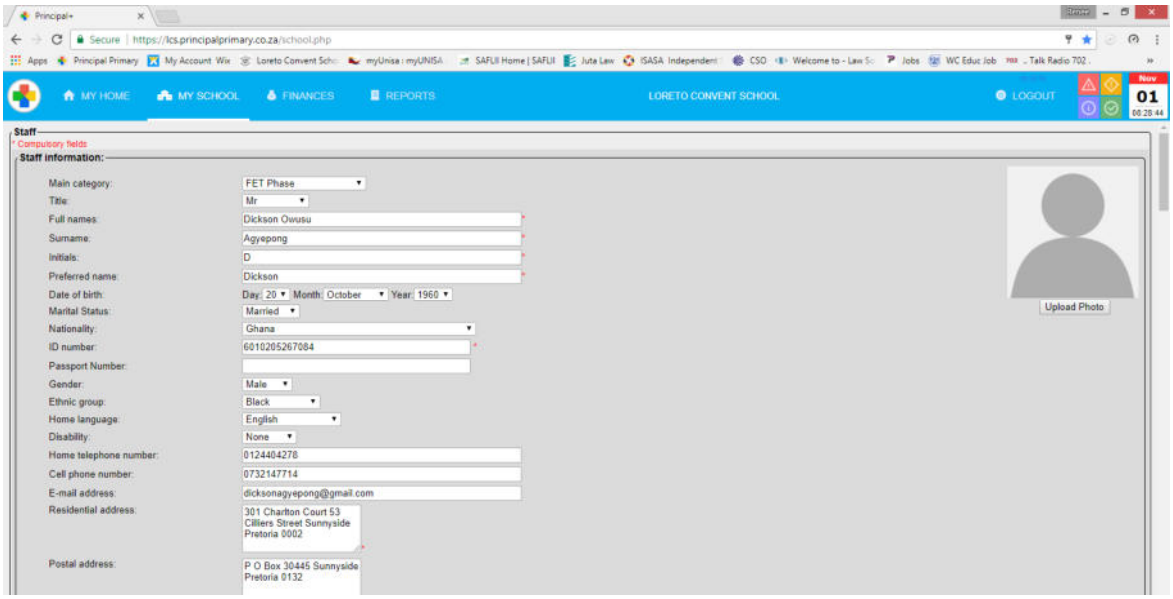
    Example of data as it is captured on PRINCIPAL PRIMARY:



STAFF INFORMATION:

1. All Information pertaining to staff is gathered in hard copy and stored in a personnel file. These files are kept under lock and key in the Principal's Office.
2. Data from these files is entered into the Data Management System (PRINCIPAL PRIMARY) so that all records are kept in electronic format as well.
3. Attendance Records are kept in the Staff Room, and staff are expected to sign in daily.
4. Staff records are kept in secure storage for 5 years after the staff member has left the employment of the school.

Example of Staff Information as it is captured on PRINCIPAL PRIMARY:



Data on the PRINCIPAL PRIMARY system can effectively be used and integrated into Department requirements and is backed up regularly. See Annexure A for the official POPI policy relating to the D6 Group - Principal Primary.

POPI ACT

A. Introduction of POPI and its meaning to schools

POPI applies to public and private entities that process the personal information of Data Subjects (the persons to whom the personal information relates). Which means that POPI also applies to schools (independent and public) when they handle the personal information of their stakeholders (learners, parents, teachers and support staff).

Loreto Convent School must comply with POPI because:

(a) It is law and POPI promotes transparency with regard to what information can be collected and how it is to be processed. This openness is likely to increase public confidence in organisations.

(b) Complying with POPI involves capturing the minimum required data on a Data Subject, ensuring accuracy and removing data that is no longer required. These measures are likely to improve the overall reliability of organisations' databases.

(c) Compliance demands identifying personal information and taking reasonable measures to protect it. Implementing such protections is likely to reduce data breaches, whose occurrences may cause reputational damage to institutions and expose them to potential legal liability.

(d) Non-compliance with POPI could expose the Responsible Party (the School) to a fine and/or imprisonment of up to 10 years (see Section 99 of the Act), depending on the nature of the infraction.

The School is required to appoint an Information Officer. The Information Officer of the School must:

(a) only undertake their duties after their school has registered them with the Information Regulator;

(b) monitor and implement Codes of Conduct issued by the Information Regulator; and

(c) encourage their school to comply with the requirements of processing personal information in terms of the provisions of POPI.

POPI also makes provision for the appointment of Deputy Information Officers to assist an Information Officer.

THE PURPOSE OF POPI

The POPI Act was signed into law on 19 November 2013 and published in the Government Gazette on 26 November 2013. This Act:

(a) recognises that a person's right to privacy includes protection against unlawful collection, retention, dissemination and use of personal information.

(b) introduces measures to protect personal information that is processed by public and private bodies.

(c) prescribes minimum requirements for processing personal information.

The main purpose of POPI is to:

(a) give effect to everyone's right to privacy as enshrined in the Constitution.

(b) facilitate the balance between the right to privacy with other rights, such as the right to access information.

(c) safeguard important interests, such as the free flow of information within the Republic and across international borders.

Within its ambit, POPI includes schools as entities that handle personal information for administrative purposes. The standards set in POPI for the protection of personal information will significantly impact upon the collection, handling and disposal of data in schools. In order to comply with POPI, schools will need to:

(a) plan and allocate resources to lawfully collect, handle and dispose of data;

(b) analyse their current practices in dealing with personal information;

(c) draft or review their own data protection policy in line with the new requirements set out in POPI; and

(d) proactively implement the requirements of POPI to enable them to avoid the pressure of meeting the compliance deadline of POPI.

B. Date of Implementation

(1) When will POPI affect independent schools?

(a) POPI was enacted in 2013 and is now an Act of Parliament.

(b) Proclamation by the President in the Government Gazette has been effected.

(c) It is important to note that the date on which the President promulgates POPI by Government Gazette will not be the POPI compliance date. The POPI Act provides a one-year compliance grace period from the date of proclamation by the President. This one-year hiatus has been provided to enable enough time for organisations to make the necessary changes for them to comply with the provisions of POPI.

(d) The means that schools will have one year to comply with the provisions of POPI.

(e) The date for compliance has been set for 1 July 2021.

C. Definitions

(1) What is 'personal information'?

Personal information is broadly defined in POPI as meaning 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, online identifier or other particular assignment to the person;

(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 personal information about the person.

(2) What is 'processing' of personal information?

Processing refers to any act that can be performed when handling personal information. POPI defines processing to include collecting, recording, organising, updating, storing, distributing, destroying or deleting personal information.

(3) What does de–identify and re–identify of personal information imply? 'De-identify' means to delete any 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.

"Re-identify" means to resurrect any information that has been de-identified.

(4) What is a Data Subject?

"Data Subject" means the person to whom the personal information relates, meaning a living person or juristic entity such as a company or institution.

(5) What is a Responsible Party?

A Responsible Party refers to a public or private body who determines the purpose, and means, of processing personal information in their possession.

(6) What is a 'record'?

A record is a form of collating information, regardless of the medium on which it is recorded, that is under the control of a Responsible Party.

D. The rights of Data Subjects

The rights that POPI bestows on learners, parents and employees to have their personal information protected by a school include the following:

In the School, a Data Subject (learner, parent and employee) has the right to:

(a) be notified that personal information about her or him is being collected;

(b) be notified that his or her personal information has been accessed or acquired by an unauthorised person;

(c) establish whether the school holds her or his personal information;

(d) request access from the school to his or her personal information;

(e) object, on reasonable grounds, to the processing of her or his personal information, including objecting to processing their personal information for purposes of direct marketing;

(f) submit a complaint to the Information Regulator regarding violations by the school to their rights to have their personal information protected; and

(g) institute civil proceedings against the school for failing to protect of their personal information.

The rights of a Data Subject established by POPI last for the duration that their personal information is in the control of the school. Loreto Convent School is required to adhere to the requirements of POPI from the time they collect a Data Subject's personal information to the time they delete or destroy that personal information.

E. Conditions for Lawful Processing of Personal Information

In order for Loreto Convent School to be compliant with POPI, there are eight (8) conditions or guiding principles that the school must comply with.

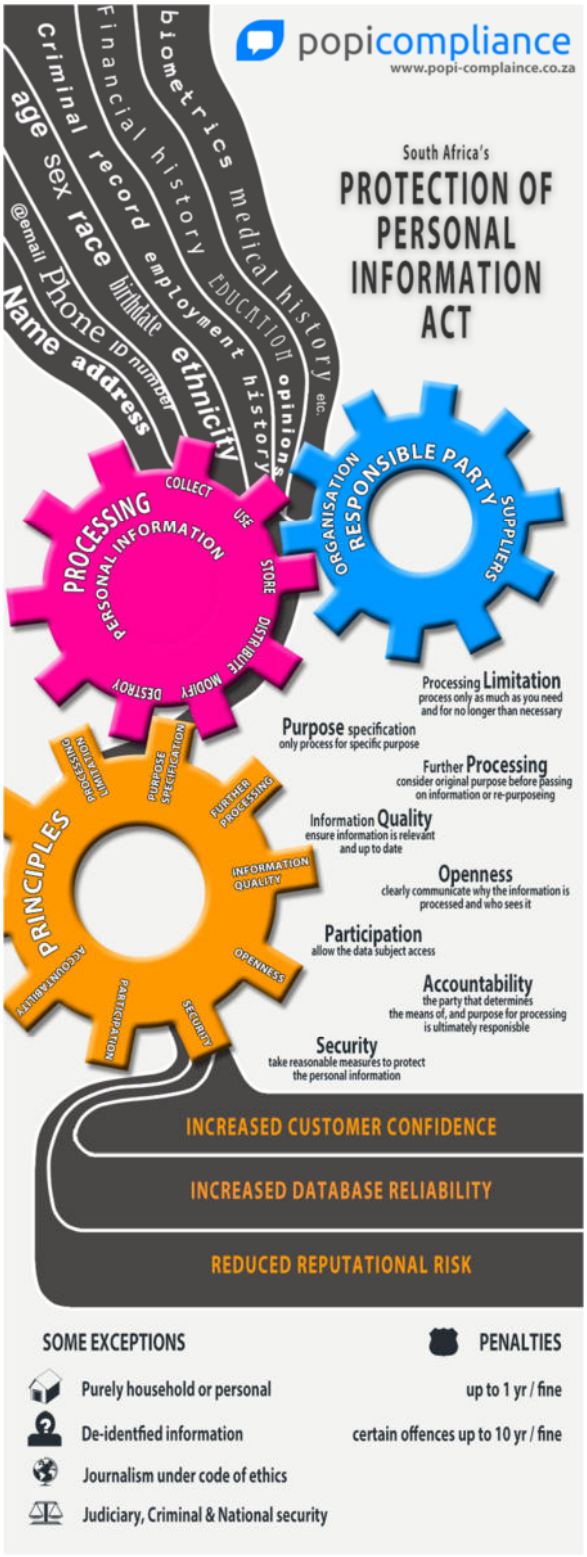
Condition 1 – Accountability:
The Responsible Party is to ensure conditions for lawful processing of information.

The school must assign responsibility for overseeing and managing compliance with POPI to a suitable person. The school is held responsible to ensure that all the eight conditions for lawful processing of personal information are met.

Condition 2 – Processing Limitation:

Personal information must be processed lawfully and in a reasonable manner which does not infringe the privacy of the Data Subject.

This means that personal information may only be processed by the school in a fair and lawful manner, that is transparent to the individual, thereby requiring the individual's explicit consent. The amount of personal information collected should not exceed its purpose.



Condition 3 – Purpose Specification:

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Responsible Party (Loreto Convent School).

This means that the school must ensure that personal information is only processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the school. Furthermore, the school must take steps to make the Data Subject aware of the purposes for which the personal information will be processed. Personal information may only be kept for as long as it is required to fulfil the purpose for which it was collected.

Condition 4 – Further Processing Limitation:

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.

This means that the school may only use personal information for those reasons that were specified at the time that the individual consented to the processing of the personal information, unless a subsequent consent is obtained from the individual.

Condition 5 – Information Quality:

Loreto Convent School must take reasonable practical steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

This means that the school must maintain the quality of the personal information. All personal information must be reliable, accurate, up-to-date and relevant to the purposes for which it was collected.

Condition 6 – Openness:

If personal information is collected, the Responsible Party must take practicable steps to ensure that the Data Subject is aware of the information being collected and where the information is not collected from the Data Subject, the source from which it is collected.

This means that the school is obliged to process information in a fair and transparent manner. Individuals must be aware of the specific personal information held about them and the purpose to which the information is being retained.

Condition 7 – Security Safeguards:

Loreto Convent School must secure the integrity and confidentiality of the personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent loss of, damage to or unauthorised destruction of the personal information or unlawful access to or processing of the personal information.

This means all personal information should be kept secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure. Password protecting personal information and putting in place policies with clear processing protocols are some of the security measures that schools can utilise in order to comply with POPI.

Condition 8 – Data Subject Participation:

Data Subjects, having adequately identified themselves, have the right to request and access information about their personal information held by the Responsible Party (Loreto Convent School). Data Subjects may also require the Responsible Party to correct or destroy personal information.

This means that individuals have the right to access and/or request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated.

Failure by the school to adhere to the above eight (8) conditions would amount to a violation of POPI.

POPI requires the school only to collect personal information for a specific purpose. The purpose for which personal information is collected, must be lawful and explicitly identified by the school. The school must make Data Subjects aware of the purpose for which their personal information is being collected.

POPI allows further processing of information but such processing must be compatible with the purpose for which the personal information was initially collected. However, further processing of personal information will not be incompatible with the initial purpose if:

(a) the Data Subject consented to further information being processed after granting their initial permission to process their information or the information is publicly available;

(b) further processing of the information is necessary to prevent or mitigate a threat to the life or health of the Data Subject;

(c) further processing of the information is necessary to comply with a legal obligation.

When augmenting personal information, the school must consider the:

(a) nature of the information;

(b) relationship between the purpose of the intended further processing and the purpose for which the information had been collected;

(c) manner in which information has been collected;

(d) consequences that the intended further processing will have on the Data Subject; and

(e) contractual rights and obligations between the parties.

The school must ensure that personal information is complete, accurate, not misleading and updated where necessary. At no charge, a Data Subject has a right to know if a school holds her, his or its personal information and to make corrections or update the personal information where necessary.

The notice from the school should inform a Data Subject about the:

(a) information being collected;

(b) purpose of why the data is being collected;

(c) consequences of not providing the personal information;

(d) existence of the right of access to, and the right to rectify, the personal information that was collected;

(e) existence of the right to object to the processing of the personal information; and

(f) right to lodge a complaint with the Information Regulator.

POPI requires the school to:

(a) secure the integrity and confidentiality of the personal information that it has in its possession or under its control;

(b) take appropriate steps to prevent the loss of, or damage to, the personal information;

(c) prevent unlawful access to, and unauthorised destruction of, the personal information;

(d) identify internal and external risks to the personal information under its control or possession; and

(e) establish and maintain appropriate safeguards against losing or damaging the personal information.

When there has been an access breach to the personal information under the school's control, the school will do the following:

(a) In the case of an access breach, the school is required to notify the Data Subject and the Information Regulator as soon as reasonably possible after the discovery of the access breach to the personal information.

(b) The school may only delay notifying the Data Subject if the Information Regulator or a public body, such as the South African Police Service, determines that notifying the Data Subject will impede a criminal investigation.

The school must give written notice to a Data Subject of an access breach to their personal information. It may send the written notification to the Data Subject by:

(a) mail at the last known physical or postal address;

(b) e-mail at the last known e-mail address;

(c) publishing a notice on the school website; or

(d) publishing a notice in the news media.

'Reasonably practicable' means that a particular provision may not have been fully complied with. However, perfect compliance is not required under the definition. In order to satisfy the 'reasonably practicable' test, the school:

(a) should be able to prove that it acted responsibly and did everything possible to reduce or eliminate risks to the personal information.

(b) needs to show that it took reasonable steps to prevent contravening the particular provisions that specifically state that 'reasonable practicable' measures must be taken to comply with that particular section.

The school bears the burden of proof to show that it did obtain consent prior to it processing the personal information of a Data Subject. Consent may be given verbally or in writing. Schools must keep a record of the consent obtained from a Data Subject.

A Data Subject may withdraw the consent they gave the school to process their personal information.

In certain instances, POPI permits the school to process the personal information of a Data Subject after they have withdrawn their consent. Outside of these exceptions, the school is prohibited from processing the personal information of a Data Subject after a Data Subject has withdrawn their consent. The school must obtain consent from the Data Subject to retain their information after they have left the school.

the school would be justified in processing the personal information of a Data Subject, without their consent, if processing the personal information:

(a) is necessary for pursuing the legitimate interest of the school or of a third party to whom the information is given;

(b) protects a legitimate interest of a Data Subject;

(c) is necessary to conclude or perform a contract to which a Data Subject is a party; or

(d) complies with an obligation imposed by law.

There are exceptions to the requirement that personal information must be collected directly from a Data Subject. It is not necessary for the school to directly collect personal information from a Data Subject if:

(a) the Data Subject has deliberately made the information public;

(b) the information is contained in or derived from a public record;

(c) the Data Subject has consented to the personal information being collected from another source;

(d) the data collection from another source will not be prejudicial to a legitimate interest of a Data Subject;

(e) the data collection from another source is necessary to maintain the legitimate interest of the

(f) responsible party or of a third party to whom the information is supplied; or

(g) receiving consent from the Data Subject would prejudice a lawful purpose of collecting the data or if getting consent is not reasonably practicable in the circumstances of the particular case.

Records of personal information should not be kept longer than it is necessary for achieving the purpose for which the personal information was collected. The school must destroy or delete a record of personal information or de-identify it after the school is no longer allowed to retain the record.

In the instance in which a school has used the personal information to make a decision regarding a Data Subject, POPI legally prescribes the period the school must retain the personal information. If a retention period is not prescribed, a school must retain the personal information for a reasonable period to grant a Data Subject an opportunity to request access to the personal information. The current time period for storage is 5 years.

Personal information must be destroyed or deleted in a manner that prevents its reconstruction or re-identification. The current best practise for the destruction of information is by shredding the document with a POPI compliant confetti shredder. Information stored digitally must be deleted in its entirety.

The school may retain personal information for a longer period than is necessary if:

(a) the Data Subject has consented to the personal information being retained;

(b) the retention of the record is required by a contract between the school and the Data Subject;

(c) the school requires the record for lawful purposes;

(d) retaining the information is authorised or required by law; or

(e) the personal information is for historical, statistical or research purposes.

In terms of the use of CCTV at Loreto Convent School, recording people amounts to processing of personal information. Which means that a Responsible Party must comply with the POPI requirements in order for the collection of images to be lawful. Data Subjects will have the right of access to the personal information processed by the school through CCTV. CCTV images should not be excessive for the purposes for which they are being collected.

The school needs to:

(a) consider if using CCTV is the most appropriate measure to use under its given circumstances and if less intrusive measures would suffice such as using security guards;

(b) decide on how it will deal with requests for access to personal information and the deletion of personal information on the CCTV; and

(c) inform people about the use of a CCTV on the premises.

The school will have to inform a Data Subject that information about them is being collected for advertising or marketing purposes. A Data Subject:

(a) may object to their personal information being used for marketing purposes or they may withdraw their consent at any time;

(b) may institute civil proceedings against a school alleging that their personal information has unlawfully been used by the school; and

(c) has a right not to be a subject of marketing.

Practically, it is recommended that the school should:

(a) not collect information unnecessarily;

(b) develop a policy for the processing of personal information;

(c) train staff on the obligations imposed by POPI when they process personal information;

(d) ensure that personal information is securely stored;

(e) keep a catalogue system to assist the school to deal speedily with requests for access to personal information by Data Subjects;

(f) have complete control over personal information kept at the school; and

(g) inform learners, parents and staff about their rights in terms of POPI.

In terms of sending data to other countries, POPI permits the transfer of data to countries that have similar standards to those established in POPI and not to countries that have lower standards than those encoded in POPI.

The school may send personal information to a country with lower data protection standards if:

(a) the Data Subject consents to the transfer;

(b) transferring the personal information is necessary for the performance of a contract between the Data Subject and the responsible party; or

(c) transferring the personal information is for the benefit of the Data Subject and if it was reasonably possible to obtain consent, the Data Subject would have granted it.

CONCLUSION:

Data Management is a vital part of the effective running of any school. At Loreto Convent School, we maintain a balance between hard copy data and electronically stored information so that we can effectively manage all records and information at the school.

In the information age, the compliance obligations imposed by POPI will likely result in better tracking and securing of the personal information that relates to parents, learners and other Data Subjects. Sound systems that protect the personal information of Data Subjects, may result in greater trust and confidence being placed in schools by parents and the general public.

It is recommended that the school therefore implement a section relating to POPI compliance in the contract signed by new parents when enrolling their children in the school, in the employment contract of staff employed at the school and in the indemnity form signed by parents yearly. It is further recommended that a POPI document be compiled that is to be distributed to all current staff, parents and learners in order to obtain consent for the storage and processing of personal information in accordance with the POPI Act. A privacy statement must be contained on the school website.

ANNEXURE A

d6 group (PTY) Ltd.
Registration Number: 2004/013738/07

PROTECTION OF PERSONAL INFORMATION POLICY

TABLE OF CONTENTS

1. DEFINITIONS

Unless otherwise stated, or the context otherwise requires, the words and expressions listed below shall bear the meanings ascribed to them:

1.1	**Applicant** – an individual who has applied to be considered for employment with the Company, or an existing employee who has applied to be considered for another position. The Applicant is the data subject as defined in terms of POPIA, being the person to whom the Personal Information or Special Personal Information relates;
1.2	**Company** – d6 group (Pty) Ltd, a Company duly incorporated in terms of the laws of the Republic of South Africa with its registered address situated at Suite 101, Block 6, Monument Office Park, 71 Steenbok Avenue, Monument Park, Pretoria, 0181;
1.3	**Deputy Information Officer** – the person identified as a deputy information officer in clause 14;
1.4	**Information Officer** – the person identified as an information officer in clause 14;
1.5	**Operator** – any third party that collects or uses Personal Information or Special Personal Information, or supports systems which contain Personal Information or Special Personal Information under the instructions of and solely for the Company or to which the Company discloses Personal Information or Special Personal Information for use or Processing on the Company's behalf;
1.6	**Personal Information** – any information or set of information that identifies or is Processed by or on behalf of the Company, as described in Chapter 1, Section 1 of POPIA;
1.7	**Policy** – this Protection of Personal Information Policy;
1.8	**POPIA** – the Protection of Personal Information Act, 2013;
1.9	**Processing** – any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including –
	1.9.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
	1.9.2 dissemination by means of transmission, distribution or making available in any other form; or
	1.9.3 merging, linking as well as restriction, degradation, erasure or destruction of information, and "Process" has the corresponding meaning;
1.10	**Regulator** – the Information Regulator established in terms of section 39 of POPIA;
1.11	**Retain** – the keeping of Personal Information in accordance with the time periods provided for in terms of the applicable legislation depending on the nature of the record, this Policy and POPIA;
1.12	**Special Personal Information** – any personally identifiable information that reveals race or ethnic origin, political persuasion, religious or philosophical beliefs, trade union membership, health or biometric information, or criminal behaviour;
1.13	**Third Parties** – third parties include but are not limited to Operators, Licensees, customers and parties providing products, goods, equipment, systems and services, such as information technology or human

	resources system suppliers, pension or retirement funds, medical aid schemes, benefits administrators or providers, human resource management administrators and payroll administrators, as well as regulatory authorities (including tax authorities and Bargaining Councils) and trade unions.

2. APPLICATION AND PURPOSE

2.1	This Policy regulates the Processing of Personal Information or Special Personal Information by the Company.	
2.2	This Policy applies to all Personal Information collected and processed by and on behalf of the Company for purposes of their business activities.	
2.3	The Company, as the responsible party in terms of POPIA, must ensure that the relevant laws relating to the Processing of Personal Information are complied with:	
	2.3.1	during the recruitment and appointment process of Applicants;
	2.3.2	during the compilation, storage and management of Personal Information relating to Applicants and the employment records of employees;
	2.3.3	for a prescribed period after the recruitment decision has been made in respect of Applicants;
	2.3.4	during the Processing of the Personal Information of employees during their employment and for a prescribed period after the termination of the employment relationship; and
	2.3.5	when Personal Information is shared with Third Parties.
2.4	The Company aims to have agreements in place with all Third Parties to ensure a mutual understanding with regard to the protection of Personal Information.	
2.5	The Company will ensure that the Policy is accessible to all employees.	
2.6	The Company has appointed an Information Officer and Deputy Information Officer to administer this Policy and ensure compliance with the provisions of POPIA.	

Part A - Human Resources

3. RECRUITMENT AND APPOINTMENT

3.1	All job advertisements sent out by the Company will set out the inherent job requirements and competency specifications for the particular vacancy, as well as the Personal Information required of an Applicant and the recruitment screening checks which will be conducted in order to Process the job application.
3.2	The Company will only consider a job application and Process Personal Information received from an Applicant if the Applicant has granted the consent as stipulated in the internal or external advertisement.
3.3	The Company will take all reasonable steps to ensure that an Applicant's Personal Information will only be Processed in order to assess whether or not the Applicant meets with the Company's employment requirements. In so doing, the Company will only Process such of the Applicant's Personal Information as

	may be necessary to make a decision on the job application. Any extraneous Personal Information supplied by the Applicant will be disregarded.

3.4	The Company will also be required to Process employees' Personal Information in connection with the employment relationship. The Company will take all reasonable steps to ensure that employees' Personal Information will only be used for purposes connected to the employment relationship.

4. RECRUITMENT AND APPOINTMENT

4.1	During the online application process or pursuant to a response received from an Applicant to an internal or external advertisement of a vacancy, the Company will collect the Applicant's Personal Information.

4.2	The Company will also need to Process Personal Information from existing employees due to changes in legislation, policies, procedures, benefits or terms and conditions of employment. Employees' Personal Information will be used for the purpose of implementing the employee's terms and conditions of employment, benefits provided to the employee, complying with legislative requirements, and generally identifying employees during the course of their employment. The Company will endeavour to obtain all of the employee's Personal Information required, directly from the employee.

4.3	The Company will take reasonable steps to ensure that an Applicant or employee understands the purpose for the Processing of their Personal Information and that informed consent is obtained from the Applicant or the employee prior to Processing any of their Personal Information.

4.4	The Company will ensure that in Processing an Applicant's or employee's Personal Information, it will adhere to its obligations in terms of POPIA.

4.5	The Company will Process an Applicant's Personal Information from the Applicant as captured in the Applicant's online profile or pursuant to the Applicant responding to an advertisement, together with such other relevant Personal Information of the Applicant which is available from a public record or has been deliberately made public by the Applicant.

4.6	The Applicant's profile as completed online or provided by the Applicant in response to an advertisement shall be directed to the Company's relevant internal department for purposes of assessing the application and the Applicant's suitability for the position applied for.

4.7	Should an Applicant furnish Personal Information which is irrelevant or beyond what is necessary in order for the Company to Process his or her application, such additional Personal Information shall not be processed as far as reasonably practicable.

4.8	The Company reserves its rights to Process Personal Information where required in accordance with any law.

5. PRE-EMPLOYMENT SCREENING CHECKS

5.1	The Company may verify the Personal Information supplied by an Applicant and conduct such other background checks as may be relevant to assess the Applicant's suitability to the position to which an Applicant applied.
5.2	The Company will conduct a reference check on Applicants who have been shortlisted for a position, in order to verify the information provided by the Applicant.
5.3	Reference checks will not be conducted in a manner that unfairly discriminates. The same reference checks will be conducted on all short-listed Applicants.

6. SPECIAL PERSONAL INFORMATION

6.1	Applicants will be notified of certain advertised positions which shall require the Company to Process the Applicant's Special Personal Information. Such positions may include positions where the Applicant would be working in a high risk area or in a position of trust.	
6.2	The Processing of Special Purpose Information must not unfairly discriminate against an Applicant or employee and the Processing of Special Personal Information must have a direct bearing on the recruitment decision.	
6.3	Special Personal Information shall only be Processed where such Processing is required in order to;	
	6.3.1	assess the Applicant's suitability for the position based on the inherent job requirements of the position to which the Applicant has applied;
	6.3.2	comply with the Company's obligations in terms of the employee's contract of employment or in relation to the provision of benefits such as medical aid, life or disability cover or retirement funding to employees.
6.4	Special Personal Information will only be Processed with the Applicant's or employee's informed consent.	
6.5	The Company will not deny employment to any Applicant solely because the Applicant has been convicted of a crime. The Company will consider the nature, date and circumstances of the offence as well as whether the offence is relevant to the duties of the position applied for.	
6.6	Should an Applicant disclose a particular medical condition or disability on his/her application, the Applicant may be required to undergo further testing to determine the Applicant's fitness for the position applied for.	
6.7	The Company will only Process the Special Personal Information of its employees where the employee has given express consent prior to the Processing or the Processing is required by law.	
6.8	Personal Information covered by medical confidentiality will be stored by Company personnel who will be bound by rules relating to medical secrecy and will be retained separately from other Personal Information.	

7. STORAGE AND MANAGEMENT OF PERSONAL INFORMATION

7.1	The Personal Information of an Applicant who successfully applies for a position within the Company and is appointed will be stored in the Applicant's personnel file on their appointment and processed as part of the employment relationship.

7.2	Should an Applicant who applied be unsuccessful in his/her application for employment, the Company will, subject to clause 11 below, store the Applicant's data for no longer than six months after the decision has been taken not to appoint the Applicant concerned. On expiry of the six month period, the Company shall destroy or de-identify the Personal Information.

8. TERMINATION OF EMPLOYMENT

8.1	The Company will not provide references to employees upon termination of employment.

8.2	Employees will be provided with the statutory certificate of service upon termination of their employment.

8.3	Upon termination of employment, the employee's Personal Information will be handed to the relevant pension or provident fund for the purposes of post-employment benefits and thereafter will be destroyed, deleted or de-identified, as legally required or in terms of this Policy and POPIA.

8.4	The Company undertakes to retain and thereafter destroy all hard copies of a terminated employee's Personal Information within such periods as are legally required from time to time or in terms of this Policy and POPIA. Such Personal Information will be destroyed on the Company's premises and in a manner that prevents its reconstruction in an intelligible form.

8.5	The Company undertakes to retain and thereafter delete or, where deletion is not reasonably possible, de-identify all soft copies of a terminated employee's Personal Information, within such periods as are legally required from time to time or in terms of this Policy and POPIA. Such deletion will be in a manner that prevents its reconstruction in an intelligible form. Such de-identification will be in a manner that prevents any association between the employee and his or her Personal Information.

Part B - Third Parties

9. DISTRIBUTION OF PERSONAL INFORMATION TO THIRD PARTIES

9.1	The Company may provide access or transfer Personal Information to Third Parties where it is necessary in the course of and for the purpose of giving effect to the Company's business activities or as required by law.

9.2	Processing of Personal Information in such circumstances would for example be for the purpose of giving effect to agreements between the Company and the Third Parties, the provision of retirement benefits, medical aid benefits, payroll and human resources administration and for the purpose of remuneration grading, salary surveys and benchmarking, procurement, supply and the provision of services.

9.3	The Company undertakes to take reasonable practicable steps to ensure that Personal Information transferred to Third Parties is dealt with confidentiality and in accordance with applicable legal requirements by those Third Parties.

9.4	The Company shall only transfer Personal Information to Third Parties in other jurisdictions where such Third Parties are subject to and comply with such laws, policies or agreements regarding privacy, data protection and confidentiality of Personal Information as may legally be required from time to time.
9.5	The Company aims to have agreements in place with all Third Parties to ensure there is a mutual understanding with regard to the protection of Personal Information, such Third Parties will be required to comply with the same or substantially similar regulations as the Company are subjected to.

10. RECEIVING PERSONAL INFORMATION FROM THIRD PARTIES

10.1	During the course of conducting its business the Company will collect Third Parties' Personal Information from time to time.
10.2	The Company will Process the Personal Information received from Third Parties pursuant to contractual arrangements and legislative requirements.
10.3	The Company will take reasonable steps to ensure that Third Parties understand the purpose for the Processing of their Personal Information and that informed consent or contractual agreement is obtained from such Third Parties prior to Processing any of their Personal Information.
10.4	The Company will ensure that in Processing a Third Party's Personal Information, it will adhere to its obligations in terms of POPIA.
10.5	With the necessary consent, the Company may also supplement the information provided with information it receives from Third Parties to ensure the accuracy of information.

General

11. REVIEW OF PERSONAL INFORMATION AND REVOCATION

11.1	The Company will verify periodically, but at least bi-annually or as legally required that the Personal Information which it has stored is accurate, up to date and complete.
11.2	The Company will provide a means for persons providing Personal Information to it to review the accuracy of the Personal Information and a means to rectify inaccurate Personal Information.
11.3	Employees must report any inaccuracies to the Information Officer or Deputy Information Officer.
11.4	Persons may revoke or withdraw their authorisation for the Processing of their Personal Information at any time by directing an email to the Information Officer or Deputy Information Officer.
11.5	As soon as a person has notified the Company that he or she has revoked or withdrawn his or her authorisation for the Processing of their Personal Information, the Company shall desist from any further Processing of the Personal Information of such person and thereafter such Personal Information will, subject to it being Retained, be destroyed, deleted or de-identified, as legally required or in terms of this Policy and POPIA.

11.6	Where appropriate persons will be made aware of potential detrimental consequences of the withdrawal or revocation of authorisation for the Processing of Personal Information.	

12. STORAGE AND MANAGEMENT OF PERSONAL INFORMATION

12.1	The Company will retain records of Personal Information for the period necessary for achieving the purpose for which the Personal Information was Processed.	
	12.1.1	Personal Information in a soft copy format is stored on the Company IT platform, including Cloud storage.

12.2	Personal Information in a hard copy format is stored as follows:	
	12.2.1	For human resources purposes, Personal Information is stored in personnel files on each site.
	12.2.2	For procurement, marketing and sales purposes, Personal Information is stored in [•].

12.3	The Company undertakes to confer an obligation on any of its management employees to maintain the Company's privacy obligations when Personal Information is distributed to managers for the purposes of management and/or business administration.

12.4	In instances where further Processing is required after the initial Processing of the Personal Information and further Processing does not correspond, as legally required, with the initial purpose of the initial Processing of Personal Information, the Company will obtain further consent from the employee, Applicant or Third Party for the further Processing of the Personal Information.

12.5	The Company will take reasonably practicable steps to ensure that all Personal Information collected is complete, accurate and not misleading, having regard to the purpose for which the Personal Information is being Processed.

12.6	The Company will take all reasonably practicable steps to ensure that all Personal Information remains confidential and is not distributed to unauthorised third parties.

12.7	Employees' Personal Information will only be made internally available within the Company to specifically authorised users, who will only have access to such Personal Information as is required for the fulfilment of their tasks.

13. STORAGE AND MANAGEMENT OF PERSONAL INFORMATION

13.1	The Company will retain records of Personal Information for the period necessary for achieving the purpose for which the Personal Information was Processed.

13.2	The Company will implement the following security measures:	
	13.2.1	The Company's Information Officer whose details are set out in 14 below is responsible for the compliance with the conditions of the lawful processing of Personal Information and other provisions of POPIA.
	13.2.2	Information Officer is assisted by the Deputy Information Officer whose details are set out in clause 14 below.

	13.2.3	Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of the employee's Personal Information, or any other action so required, in terms of POPIA.
	13.2.4	In respect of those Employees who are employed at the time the Company implements this Policy the Company will assume tacit agreement from such Employees for the use and Processing of the Employees' Personal Information for the purpose of implementing the employee's terms and conditions of employment, benefits provided to the employee, complying with legislative requirements, and generally identifying employees during the course of their employment with the Company, provided that the Company may require existing Employees to provide written permission or sign an addendum to their contracts of employment in this regard where the Company deems it necessary or appropriate.
	13.2.5	All current Third Parties of the Company will where appropriate be required to sign an addendum to their contracts with the Company containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.
	13.2.6	All electronic files or data are backed up by the Company's IT department who is responsible for system security which protects third party access and physical threats.
	13.2.7	An Incident Register will be kept to log any security incidents and to report on and manage said incidents this register will be maintained by the Information Officer.
	13.2.8	The Company's Information Officer and the IT department shall identify all reasonably foreseeable internal and external risks to Personal Information, establishing and maintaining appropriate safeguards against the risks identified, regularly verifying that the safeguards are effectively implemented, and ensuring that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
	13.2.9	Applicants will be informed should their Personal Information be accessed or acquired by any unauthorised person.

14. INFORMATION OFFICER

The Company will appoint an Information Officer and Deputy Information Officer under the Company. The details are as follows:

Information Officer Details	Patric Trollope
Physical Address:	Suite 101, Block 6, Monument Office Park 71 Steenbok Avenue, Monument Park Pretoria, 0181
Postal Address:	P.O. BOX 25190 Monument Park 0105
Telephone No:	087 820 0088
Fax No:	086 536 7148
Email Address:	patrict@d6ed.co.za

Deputy Information Officer Details	
Physical Address:	Suite 101, Block 6, Monument Office Park 71 Steenbok Avenue, Monument Park Pretoria, 0181

Postal Address:	P.O. BOX 25190 Monument Park 0105
Telephone No:	087 820 0088
Fax No:	086 536 7148
Email Address:	

15. AMENDMENTS TO THIS POLICY

This Policy may be amended on commencement of POPIA in its entirety insofar as there are substantive amendments to POPIA from its current form, pursuant to any amendments to POPIA or changes to the law relating to Personal Information and on publication of the regulations under POPIA insofar as this may be necessary from time to time.