



Solid Foundations Primary School

Data Management Policy (2023/11)

1. Data protection principles

In accordance with the PoPI Act of South Africa (November 2013) the school recognises the importance of maintaining the privacy of staff, pupil and family records and information and endeavours to follow the 8 principles set forth by the Protection of Personal Information Policy (November 2013) namely:

- 1.1.1. Accountability
- 1.1.2. Processing limitation
- 1.1.3. Purpose specification
- 1.1.4. Further processing limitation
- 1.1.5. Information quality
- 1.1.6. Openness
- 1.1.7. Security safeguards
- 1.1.8. Data subject participation

2. Data sharing and access request approach

- 2.1. Public Data Subject Access Request (DSAR) can be made at the front office.
- 2.2. DSAR is subject to identity verification before requests are approved.
- 2.3. Teachers' email addresses and telephone numbers may not be given to parents unless the teacher has specifically decided to do so.
- 2.4. Class lists with children's names and surnames may not be publicly shared.
- 2.5. No telephone numbers, email addresses or any other personal information of teachers, parents or pupils may be given to a third party under any circumstances.
- 2.6. The teacher reserves the right to either give the learner's workbook back to the learner at the end of a school year or to retain the workbooks. It is encouraged that workbooks are returned to pupils and any assessment activities that are to remain confidential be removed from the workbooks and shredded prior to the child taking them home.

3. Paper records of Personal Information

- 3.1. Paper records of personal information are kept in a secured cupboard when not in use. This includes mark books and class lists.
- 3.2. When the retention period for paper records of personal information expires or copies are no longer necessary, these records are destroyed by shredding.

- 3.3. Paper records awaiting shredding are kept in a secure paper records box that is only accessible by the Information Officer or principal.
- 3.4. Once read, all psychology, therapy and remedial specialist reports pertaining to pupils are filed in their Learner Profiles immediately. Reports may not be left where they can be read or accessed publically.
- 3.5. Shredding occurs continuously in the office, or papers to be shredded are kept in a locked box until shredding occurs.

4. Requirements for transporting Personal Information

- 4.1. When paper records of personal information (e.g. learner profiles) need to be transported off of school premises, this data is secured in a sealed envelope.
- 4.2. All such records are either hand delivered by a member of staff or couriered.

5. Management review procedures

- 5.1. The Information Officer does a Data Impact Analysis whenever:
 - 5.1.1. The school begins utilizing new administration systems, software or technology that make use of personal information.
 - 5.1.2. Participating in a high-risk activity.
 - 5.1.3. Processing large amounts of special information.
- 5.2. The Information Officer will investigate any incident where a data breach seems to have occurred and data subjects will be informed if their data has been lost, destroyed, or otherwise mishandled, following internal investigation procedures.

6. Retention period for personal information

- 6.1. Staff data is retained for 4 years.
- 6.2. Student, parent/guardian, next of kin, and designated emergency information is retained for 10 years.
- 6.3. Personal Information may be retained longer if the school is required to do so by another governmental agency (e.g. SARS).
- 6.4. Student assessments are retained for 2 weeks after the report cycle they contributed to. If no parent queries have been made as to the mark, assessments may be destroyed.