Personal Information Assessment Report

An assessment was completed to help identify and minimise the data protection risks from processing personal information.

POPIA applies when the personal information of a living person or existing entity is processed (the latter term being very widely defined under POPIA to include collection, recording, organising, collating, distributing, modifying, storing, using and destruction) by a responsible party (which is a public or private body, or any other person which alone or together with others determines the purpose of and means for processing).

1. **Jumping Fox Software - Responsible Party**

A responsible party is the person who determines the purpose of and means for processing of personal information.

It applies only to the processing of personal information if the data are entered into a record by or for a responsible party by making use of automated or non-automated means, where the responsible party is domiciled in South Africa. If the responsible party is not domiciled in South Africa, POPIA applies if that responsible party makes use of automated or non-automated means in South Africa, unless those means are used only to forward personal information through South Africa.

Jumping Fox Software is a responsible party in respect of the personal information that it processes in relation to its employees and clients.

Responsible person per department

1. Information Officer

   Daleen Vorster

   Daleen@jumpingfoxsoftware.com
2. Business Growth Department

   Hendrik Snyman

Hendrik@jumpingfoxsoftware.com

3. Head of Development

   Riaan Dreyer

   Riaan@jumpingfoxsoftware.co.

4. Bookkeeper

   Karen Hermanus

   Accounts@jumpingfoxsoftware.com

POPIA contemplates that the responsible party is the one that remains ultimately accountable for the information being processed by the operator, and provides that the responsible party must secure 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, damage to, or unauthorised destruction of personal information and unlawful access to or processing of personal information.

This means that the responsible party must ensure that an operator or anyone processing personal information:

• only does so with the knowledge or authorisation of the responsible party; and

• treats personal information which comes to their knowledge as confidential and does not disclose it, unless required by law to do so or in the course of the proper performance of their duties

A responsible party must therefore, in terms of a written contract between the responsible party and the operator, ensure that the operator that processes personal information for the responsible party establishes and maintains the security measures as prescribed under POPIA.

Assessment - Personal Information Flow

1. Employees

OneDrive

Employee contracts and personal information are stored on OneDrive, cloud storage platform, under the Operations folder of the director Daleen Vorster. The people who have access to the specific folder is Daleen and the IT company assisting with IT infrastructure, One2One (admin).

Employees make use of OneDrive to manage their internal work. Employees choose their own passwords and the process complies with the guidelines set out in the JFS password policy.

Access to the OneDrive folder is only possible by entering a username and password. OneDrive comes with built-in security features, including data encryption both in the cloud and on any connected device.

Pastel

Employee information is necessary for payment of monthly salaries are saved on Pastel, a cloud storage platform. The people who have access to the information is the company bookkeeper Karen Hermanus and Daleen Vorster. Access to the Pastel system is only possible by entering a username and password. Employees receive salary slips per email.

Microsoft 365

The company emails are setup using Microsoft 365 that gives advanced protection from viruses and cybercrime.

A risk assessment was done on the installation of the software, to ensure professional and risk-free installation.

Information on installation risk levels is set out in Annexure “A” attached to the report.

LastPass

The username and passwords are stored by Daleen Vorster on LastPass and only Daleen has access to the LastPass passwords.

Possible Risk

Not all employees store OneDrive passwords on a password manager.

Risk Prevention

All employees must make use of a password manager to keep office passwords safe.

2. Clients

License Agreement

Client license agreements and personal information are stored on OneDrive, cloud storage platform, under the Sales folder. The people who have access to the specific folder is company director Daleen Vorster, the IT company that assists with the IT infrastructure, One2One (admin), and Riaan Dreyer, head of development.

OneDrive comes with built-in security features, including data encryption both in the cloud and on any connected device.

Client Contact List

A client list contains the school's name and contact number, the user's name and surname, the email address and in some cases the mobile number. The information is necessary in order to perform support and customer success duties and for invoicing purposes. The client list is saved on the Jumping Fox Software system (server Xneelo).

Microsoft 365

The company emails are setup using Microsoft 365 that gives advanced protection from viruses and cybercrime.

JFS Website

Client data is uploaded to the JFS account management, exemption and corporate business systems when the client is setup for access to the system. The process clients follow when providing personal information and other data files for setup purposes is detailed in Annexure "B" attached to the report.

Clients get access to the site with a username and password. The requirements set out in the company password policy have been updated as Jumping Fox Software has not renewed its license as a credit bureau re-seller.

The hosting company where the client information is stored is Xneelo.

Available information on Xneelo's compliance with the POPI Act regulations.

https://xneelo.co.za/help-centre/products-and-services/data-protection/

System Need Help Functionality

Clients provide personal information when requesting support via the system "need help" functionality.

The process clients follow when requesting support is detailed in Annexure “C” attached to the report.

System Backups

Client personal information, data files and documents are backed-up on a weekly basis.

Multiple passwords are involved in the backup process:

- The Backup PC password
- Each site’s database password (excluding the exemption system since this is managed from firestore/google cloud services).
- Each site’s server credentials (excluding the exemption system since this is managed from firestore/google cloud services).

The backup processes the development team follows are detailed in Annexure “D” attached to the report.

Pastel

Client information is necessary for invoicing purposes and are saved on Pastel, a cloud storage platform. The people who have access to the information is the company bookkeeper Karen Hermanus and Daleen Vorster. Access to the Pastel system is only possible by entering a username and password. Employees receive salary slips per email.

Pastel has upgraded security features to be POPI compliant. (See website)

Mailchimp

Jumping Fox Software uses MailChimp to send out emails to clients in batches. The content of the emails relates to system updates and other important notification.

Jumping Fox Software has one login account shared by Johan Nel and Daleen Vorster. The login details are saved on Google Password Manager and LastPass. Jumping Fox Software has Two-Factor Authentication setup on our MailChimp account so every time someone tries to login an SMS is sent to the accountholder’s mobile phone.

Possible Risk

Clients share personal information, other data files and license fee agreements via email.

Employees share data files via email.

Monitoring of client password reset.

The site backup uses FTP and files are not encrypted during the transmission.

Risk Prevention

Educate clients on the correct process to follow when transferring personal information and data files.

Amend internal process on data file transfers.

Update process to ensure clients update passwords.

Consider using a VPN to ensure all site backup's transmissions are always encrypted regardless of the stream. The future backup plan includes newer infrastructure around the backup system, rebuilding to a server PC and using it to automate the backup process. This would include licencing for the Database backups and providing automated responses via email when backups are complete, or if they fail. Also consider introduced Synology's NAS (Network Attached Storage) to keep an off-site backup of all our files (including the one Drive) for easy access to backed up files. By doing so we follow part of the 3-2-1 Backup rule. The venerable 3-2-1 rule for backing up data remains a tried-and-true method for ensuring the integrity of copied data that is essential to disaster recovery efforts.

Security advantages of using the following tools:

- Different storage – Using a different storage type than what you use for your primary storage. An attack designed for one will probably not work on another.
- Different environment – Using a backup system that isn't directly reachable via your LAN. That's another way to prevent compromised on-prem servers from attacking your backups.
- Different OS – Using a backup server or service that runs on an OS other than Windows can go a long way. Most ransomware attacks have been against Windows.
- Different account – Using completely different credentials in your backup and disaster-recovery systems. That way if an account is compromised, the credentials won't work to attack your backups.
- Immutable storage – Some cloud vendors offer immutable storage, where backups sent there cannot be changed or deleted until the time you specify. Even you can't delete them.

2. Jumping Fox Software - Operator

Section 1 of POPIA defines an operator as “a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party”. In other words, an operator is a person or entity that is contracted by another person, the responsible party, to assist with the processing of personal information for such responsible party.

Jumping Fox Software is an operator in respect of personal information they process on behalf of a responsible party, the clients of Jumping Fox Software. The processing of the data is done in terms of a mandate set out in a license agreement.

Clients sign the license agreement to gain access to the debtor managements, exemption, or corporate business systems.

<u>Debtor Management Solution</u>

The system is available to schools to assist in the management of debtor accounts and collection of outstanding school fees.

The information transferred from the school's financial system to the debtor management system includes the parent’s name and surname, Id number, physical address, email address and mobile number. The data transfer is done manually or via an API. The data files are known as a master file, detailed ledger, and age analysis.

When an account completes all the workflow steps the account can be handed over to attorneys for the collection of the outstanding school fee account.

The system provides for two factor authentication when a user logs into the system.

The process clients follow when providing personal information and other data files for setup purposes is detailed in Annexure “B” attached to the report.

The authentication process users follow are detailed in Annexure “E” attached to the report.

Continuous system maintenance and testing is part of the development team’s daily routine. The testing and maintenance plan is set out in detail in “Annexure F” attached to the report.

Possible Risk

Expiration of passwords

Risk Prevention

Update the system to include password expiration and follow a maintenance plan on continuous testing of the first point of entry.

Continuous system maintenance. The testing and maintenance plan is set out in detail in "Annexure F" attached to the report.

Exemption System

The system is available to schools to assist with the processing of applications for exemption from payment of school fees.

The parent applies for exemption by completing an online exemption application form. The information the parent is required to complete includes the parents and learner name and surname, ID numbers, other dependent's name and surname, grades, physical address, email address, mobile number, income, and expenses.

Information can also be transferred from the debtor management system to the exemption system. The personal information includes the parent's name and surname, ID number, learner name, surname and ID number and grade. The data transfer is done via an API.

When the application process is completed, the detail remains on the system as the parent can again apply for exemption the next year.

Personal information is processed to approve or deny an application for exemption from payment of school fees.

Detailed information on the system security, two factor authentication and cross border transfer of data is set out in Annexure "G" attached to the report.

Continuous system maintenance and testing is part of the development team's daily routine. The testing and maintenance plan is set out in detail in "Annexure F" attached to the report.

Possible Risk

Staff access to all personal information.

Risk Prevention

Improve permission levels and review system activity log on a continuous basis.

Continuous system maintenance. Continuous system maintenance. The testing and maintenance plan is set out in detail in “Annexure F” attached to the report.

Corporate Business System

The system is available to businesses to assist in the management of debtor accounts and collection of outstanding accounts.

The information transferred from the business financial system to the debtor management system includes the accountholder name and surname, Id number, physical address, email address and mobile number. If the accountholder is an entity the registration number and registered address is imported. Details of other stakeholders can also be imported if the business owners use the information in the management of debtor accounts.

The data transfer is done manually or via an API. The data files are known as a master file, detailed ledger, and age analysis.

When an account completes all the workflow steps the account can be transferred to attorneys for the collection of the outstanding school fee account.

The system provides for two factor authentication when a user logs into the system.

The process clients follow when providing personal information and other data files for setup purposes is detailed in Annexure “B” attached to the report.

The authentication process users follow are detailed in Annexure “E” attached to the report.

Continuous system maintenance and testing is part of the development team’s daily routine. The testing and maintenance plan is set out in detail in “Annexure F” attached to the report.

Possible Risk

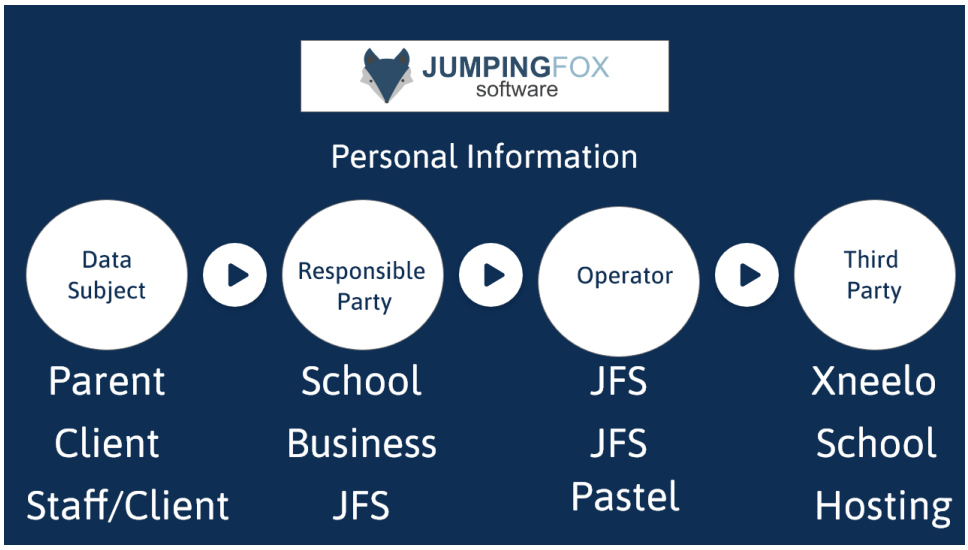
Expiration of passwords - to ensure that a balance is maintained between security and user accessibility, we recommend that we do not include the expiration of passwords within the scope of the two-factor authentication security update.

Risk Prevention

Include password expiration as part of the authentication process and follow a maintenance plan on continuous testing of the first point of entry.

Continuous system maintenance. Continuous system maintenance. The testing and maintenance plan is set out in detail in “Annexure F” attached to the report.

3. Personal Information Flow Chart



Jumping Fox Software has the role of a Responsible Party towards staff and clients and the role of Operator when rendering a service (SaaS) in the management of debtor accounts and collections.

4. Role of Information Officer

The Promotion of Access to Information Act (PAIA) automatically designates a person in each organisation as an Information Officer and therefore, by default, every organisation in South Africa has such an officer. (The officer performs the same role as a Data Protection Officer under the GDPR.)

The information officer is responsible for ensuring that the organisation complies with POPIA and accordingly his or her additional duties include the following:

• encouraging compliance with conditions for the lawful processing of personal information

• dealing with requests made pursuant to POPIA (presumably by the Information Regulator or data subjects)

• working with the Regulator on investigations conducted in relation to prior authorisations (pursuant to Chapter 6 in relation to the body)

• otherwise ensuring compliance by the body with the provisions of POPIA

• developing, implementing, and monitoring a compliance framework

• seeing to it that a personal information impact assessment is done to ensure that adequate measures and standards exist

• developing, monitoring, and maintaining a PAIA manual and making it available

• developing internal measures and adequate systems to process requests for access to information and

• ensuring that internal awareness sessions are conducted.

The officer is responsible for ensuring that the organisation complies with PAIA. An information officer of a responsible party (or body) must:

• encourage and ensure compliance with PAIA in accordance with the body's definition of compliance

• create, maintain, and update a PAIA manual for the body,

• evaluate and approve requests for access to information received in terms of the grounds set out in PAIA, within the time constraint or any extended period.

5. Role of Information Regulator

POPIA introduces and provides for the establishment of an independent supervisory authority, namely the Information Regulator, specifically established for the purpose of data protection.

6. Employee awareness checklist

Employees must receive continuous training on the requirements of the POPI Act. Employees must also have knowledge of the different company policies in order the implement and maintain the required measures.

Attached to the report are copies of the company policies: (Annexure H – Q)

1. Data transfer policy
2. New client onboarding process
3. Information security process
4. Disaster management data recovery plan
5. Data retention
6. Data handling
7. Data access and prescribed purposes

8. Complaints and disputes
9. Change management
10. Business continuity and succession plan

A data subject has certain rights when it comes to the processing of personal information. A checklist per category is attached to report as Annexure “R - X”:

1. Right to access
2. Right to data portability
3. Right to erasure
4. Right to rectification
5. Right to restrict processing
6. Right to related automated decision-making
7. Right to be notified

Monthly review sessions will take place to discuss the system maintenance reports, identify and review risks and update company policies and processes.

Daleen Vorster is the registered Information Officer of Jumping Fox Software. A copy of the registration document is attached to the report as Annexure “Y”.