2021

a|CITY CHURCH

DATA PROTECTION POLICY & PROCEDURE JULY 2021

Debbie Sloane

POPIA
(Protection of Personal Information Act)

ABBREVIATIONS USED

OTL- Operational Team Leader
PI- Personal information
ELT- Executive Leadership Team
IO- Information Officer
DIO- Deputy Information Officer
O- Operator
DS- data subjects

CONTENTS PAGE

INTRODUCTION
DEFINITIONS

Personal Information means information relating to an identifiable, living, natural person, identifiable, existing juristic person, including, but not limited to—

- Information relating to the race, gender, national or social origin, language, age disability;
- Information relating to the education or medical or financial history of the person;
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinion, views, or preferences of the person;
- 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;
- The views or opinions of another individual about the person; and
- 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 information about the person.

KEY DETAILS

- Policy prepared by D.A. Sloane
- Approved by Executive Leadership Team members on: 13 June 2021
- Policy became operational on: 1 July 2021
- Next review date: 1 September 2021

INTRODUCTION

a|CITY CHURCH needs to gather and use certain information about individuals.

These can include guests, suppliers, volunteers, employees, and other people the church has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, and stored to meet the church's protection standards — and to comply with the law.

WHY THIS POLICY EXISTS

This data protection policy ensures a|CITY CHURCH:

- Complies with data protection law and follow good practice;
- Protects the rights of staff, guests, and volunteers;
- Is open about how it stores and processes individuals' personal information;
- Protects itself from the risks of a data breach.

POPI: APPLYING THE ACT TO a|CITY CHURCH

Within "the church" context, the purpose of the POPI Act is to safeguard the personal details of members and those visiting the church. It is for this very reason that the church needs to put suitable controls in place to ensure that this is maintained at all times and regularly accessed.

a|CITY CHURCH treats all personal information as if it were "for your eyes only."

A. <u>THE POPIA IN RELATION TO a|CITY CHURCH</u>

1. a|CITY CHURCH has a Personal Information Inventory that lists all the areas where the following information is required from guests; volunteers & staff
    - Demographic information;
    - Contact information;
    - Preferences;
    - Background information

    This inventory includes special personal information that requires extra care
    - Criminal record;
    - Sexual orientation;
    - Client information obtained during counselling.

2. In terms of point 1 above, the a|CITY CHURCH has relevant policies (course of action), procedures (official step by step way of doing something) in place so safeguard the recording, storage & use of personal information.

3. There are specific processes for handling and protecting personal information.

4. Existing processes are reviewed regularly, and the necessary gaps addressed.

5. In terms of all online platforms, there is a suitable firewall in place to ensure the safe keeping, storage, and processing of ALL data.

B. MORE ABOUT POPI

POPI enshrines section 14 of the Constitution of the Republic of South Africa, 1996. This states that everyone has the right to privacy, which includes a right to protection against the unlawful collection, retention, distribution and use of personal information.

In essence, POPI strives to:

1. Promote the protection of personal information processed by public and private bodies (including churches);
2. Introduce information protection principles, to establish the minimum requirements for the processing of personal information; and
3. Make provision for the rights of people regarding unwelcome electronic communications and automated decision making.

When it comes to the processing of special personal information…

1. **POPI section 25:** In general, there is a ban on the processing of special personal information e.g. a person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour.

2. **POPI section 26:** The church is however exempted and therefore has the right to process information concerning their members or employees or other persons belonging to the institutions religious or philosophical beliefs.

3. **POPI section 28:** While churches might be exempted from processing their members religious or philosophical beliefs, they still have an obligation to protect other 'personal information' of the member i.e. How churches will safeguard members and visitor's personal information.

C. 8 IMPORTANT PROTECTION PRINCIPLES ADHERED TO BY a|CITY CHURCH

1. Accountability

POPI section 7: The church has designated a "Responsible Person" to give effect to the eight POPI principles and ensure that the principles set out and all the measures that give effect to the principles are complied with. POPI accountability ultimately lies with the Senior Pastor. This role is delegated to the designated Responsible Person(s).

2. Process Limitations

2.1 **POPI section 8:** Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of any individual. Therefore, due care must be taken over e.g. First Time Welcome Cards, altar call decision cards, prayer point cards (if including names), Tithe envelopes (if including names) etc. Completed cards must be always kept in a secure place, viewed only by those required/designated and discarded with care e.g. shredding

2.2 **POPI section 9:** Personal information may only be processed for the purpose it was intended for, provided that the information is relevant and not excessive e.g. a prayer request card is not a source for getting member names and or details for any other purposes. In essence, if you want personal information, rather use a connect card.

2.3 **POPI section 10:** Personal information may only be processed if **(a)** the person concerned consents to the processing; **(b)** it is necessary to carry out relevant ministry related duties such as follow-ups, invitations, reporting etc.; or **(c)** if it complies with an obligation imposed by law on the responsible party. It is important to note that a person may object at any time, on reasonable grounds, to the processing of personal information e.g. when a member chooses

to or stops being a member. Where or when a person has objected to the processing of personal information, the church should no longer process the personal information.

2.4 **POPI section 11:** Personal information must be collected directly from the persons concerned when they come to church or any of its outreach programmes It is fine if the information is contained in a public record or has deliberately been made public by the person concerned. In churches with more than one campus or where churches form part of a larger structure such as the Assemblies of God Group, it is imperative that everyone be made aware of this and that they consent to the passing on the information.

3. Purpose Specification

3.1 **POPI section 12:** Personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the church. More so, the member or person concerned must be aware of the specific purpose the church is collecting information. Getting people to provide information in exchange for something of value to them would not be appropriate. This includes using decision cards for the purpose of membership record or similar.

3.2 **POPI section 14:** It is imperative that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently used. In terms of membership or where minors need to be signed in for security reasons, people need to consent to the retention of the records. The church must establish appropriate safeguards against the records being used for any other purposes.

3.3 Where information retention may be required or prescribed by law or a code of conduct such as when a church stores banking details e.g. debit orders, debit, or credit card details, then the church must also establish appropriate safeguards.

4. Further Processing Limitations

4.1 **POPI section 15:** The further processing of personal information (where such information has been saved on a database or spreadsheet) must be compatible with the purpose for which it was collected in terms of point 3 directly above.

4.2 The church's "Responsible Person" must always consider the following; (a) make sure that the person concerned has given consent to process their information, (b) whether the member has not requested deletion prior to processing their information and (c) whether the information is compatible with the purpose of collection, available in a public record.

5. Quality of Information

5.1 **POPI section 16:** The church's "Responsible Person" must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary for the purpose it is intended.

6. Openness

6.1 **POPI section 17:** Personal information collected as part of membership or any transaction should include a name, address or contact detail such as an email address. This is to be collected in a fair and transparent manner. To ensure that the processing of information is fair, individuals must be aware of what specific personal information is being held by the church.

6.2 **POPI section 50:** Section 17 read in conjunction with section 50, mandates the church to 'register' by submitting a notification to the Regulator before commencing the processing of personal information. Details of the notification content are stipulated in section 51.

7. Security Safeguards

7.1 **POPI section 18:** The church through the "Responsible Person" must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures.

7.2 Appropriate internal control measures must be in place and regularly evaluated i.e. ensuring that security practices and procedures are effective and in place.

7.3 **POPI section 19:** All employees and volunteers processing personal information on behalf of the church must always, (a) process this information with the knowledge or authorization of the church; and (b) treat personal information which comes to their knowledge as confidential and must not disclose it.

7.4 **POPI section 21:** Should there be a breach (unauthorized access to record or any other related compromise), the church must notify the POPI Regulator, and the person/s affected as soon as is reasonably practicable. It is also essential to consider the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the church's information system.

7.5 A notification must provide sufficient information to allow the affected person/s to take protective measures against the potential consequences of the compromise, including, if known to the church, the identity of the unauthorized person who may have accessed or acquired the personal information.

8. Personal Information on Record and 3rd. Party Disclosures

8.1 **POPI section 22:** The church must make provision for the members, who have provided adequate proof of identity, to request what personal information the church holds about them, including third parties the church may have shared the member's personal information with.

WHY THIS POLICY IS IMPORTANT

a|CITY CHURCH is committed to processing data in accordance with its responsibilities in accordance with THE POPIA.

Personal Information shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

RESPONSIBILITIES OF STAFF & VOLUNTEERS AT a|CITY CHURCH

Everyone who works for or at with a|CITY CHURCH has some responsibility for ensuring data is collected, stored, used and handled appropriately.

Each team that handles personal information must ensure that it is handled and processed in line with this policy and personal information protection principles.

However, the following people have key areas of responsibility:

EXECUTIVE LEADERSHIP TEAM

John Sloane, Debbie Sloane, Hilton Mentor, Ricky White, Len White, Carla Delport, Fiona Erispe, Rocky Likuba

- Is ultimately responsible for ensuring that a|CITY CHURCH meets its legal obligations.

INFORMATION OFFICER

Debbie Sloane

The Information Officer is responsible for:

- Keeping the Executive Leadership Team updated about personal information protection responsibilities, risks, and issues.
- Reviewing all personal information protection procedures and related policies, in line with an agreed schedule.
- Arranging personal information protection training and advice for the people covered by this policy.
- Handling personal information protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the personal information that the church holds on them.

In addition, according to POPI Regulations 2018: Responsibilities of Information Officers

Regulation 4:

An Information Officer must, in addition to the responsibilities referred to above, ensure that:

- A compliance framework is developed, implemented, monitored, and maintained;
- A personal information impact assessment is done to ensure that adequate measures and standards exist to comply with the conditions for the lawful processing of personal information;
- A manual is developed, monitored, maintained, and made available as prescribed in s14 and s51 of the PAIA Act;
- Internal measures are developed together with adequate systems to process requests for information of access thereto; and
- Internal awareness sessions are conducted regarding the provisions of the Act, codes of conduct, or information obtained from the Regulator.
- The Information Officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

POPI Act: Section 56: Designation and delegation of deputy Information Officer 9s)

- Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of:
    - Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of the Act; and
    - Any power or duty conferred or imposed on an information officer by this Act to a deputy Information Officer of that private of public body.

IT ADVISORY TEAM

Ricky White, IT Naledi

The **IT Advisory Team** is responsible for:

- Ensuring all systems, services and equipment used for storing personal information meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the church is using to store or process personal information. For instance, cloud computing services.

MARKETING TEAM

Carla February, Ethan White, Zama Moloi

The **Marketing Team** is responsible for:

- Approving any personal information protection statements attached to communications such as emails and letters.
- Where necessary, working with other staff & volunteers to ensure marketing initiatives abide by personal information protection principles.

DEPUTY INFORMATION OFFICERS

Carla Delport, Fiona Erispe

The **Deputy Information Officer's** responsibilities:

- Educating volunteers on the POPIA compliance regulations;
- Training staff & volunteers involved in data subject access requirements and request processing;

- Conducting audits to ensure that compliance requirements are being met;
- Serving as a key point of contact with the IR;
- Monitor the data protection efforts;
- Define privacy and data protection policies & practices;
- Respond to requests made by data subjects to de- consent or to update PI within 72 hours;
- Interfacing with data subjects regarding their privacy rights.

OPERATOR

Zama Moloi

The **Operator's** responsibilities:

- Maintain records of all data processing activities;

WHO THIS POLICY APPLIES TO?

This policy applies to:

- All staff, guests, and volunteers of a|CITY CHURCH;
- All contractors & suppliers working on behalf of a|CITY CHURCH.

It applies to all personal information that the church holds relating to identifiable individuals. This includes:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Mobile phone contact details
- Life stage & age
- …plus any other information relating to individuals

PERSONAL INFORMATION RISKS

This policy helps to protect a|CITY CHURCH from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the church uses data relating to them.

- Reputational damage. For instance, the church could suffer if hackers successfully gained access to personal information.

GENERAL STAFF & OPERTIONAL TEAM LEADER GUIDELINES

- The only people able to access personal information covered by this policy should be those who need it for the specific task assigned to them. For example OLT, ACC (pastoral care) uses personal information to contact & pray for guests weekly.
- Personal information should not be shared informally. When access to confidential information is required that falls outside the parameters of OTL who require access to personal information for church related business matters, staff & volunteers can request it from the Information Officer.
- The Information Officer will provide training to all OTL's to help them understand their responsibilities when handling personal information.
- Employees keep all data secure, by taking sensible precautions and following the guidelines below:

  Strong passwords must be used, and they should never be shared.

  Personal data should not be disclosed to unauthorized people, either within the church or externally.

  Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

  Employees should request help from the Information Officer if they are unsure about any aspect of data protection.

HOW YOUR INFORMATION IS STORED

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Advisory Team or the Deputy Information Officer.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer, in an exposed filing shelf.

- Data printouts should be shredded and disposed of securely when no longer required. Shredding is done using the office paper shredder device.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts through the following protective measures:

- Data should be protected by strong passwords that are changed regularly and never shared between employees & OTL.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used in the filing cabinet in the lead pastor's office.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- All computers and laptops used for data subject storage purposes
    - must have updated antivirus programmes;
    - must have a BitLocker encryption key;
    - all passwords stored in a centralized password control vault that requires authentication in order to access (2Factor Authentication)

HOW YOUR INFORMATION IS USED

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT Advisory Team can explain how to send data to authorized external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

HOW YOUR INFORMATION IS UPDATED

Reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Employees should not create any unnecessary additional data sets.
- Employees should take every opportunity to ensure data is updated.
- a|CITY CHURCH will make it easy for data subjects to update the information the church holds about them. For instance, via the church website.
- Data should be updated as inaccuracies are discovered. For instance, if a guest can no longer be reached on their stored telephone number, it should be removed from the database & the updated number added. Similarly guests can update their info via a link on the website.
- It is the marketing team's responsibility to ensure that links are functional and that all the required PI is stored and accessed by authorized personnel.

YOU CAN ACCESS YOUR INFORMATION

All individuals who are the subject of personal data held by a|CITY CHURCH is entitled to:

- Ask what information the church holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the church is meeting its data protection obligations.

If a data subject contacts the church requesting this information, this is called a data subject access request.

Data subject access requests from individuals should be made by email, addressed to the DIO at admin@acitychurch.co.za or on the digital platform https://bit.ly/aCITYSubjectDataRequest

The DIO will aim to provide the relevant data within 72 hours.

The DIO will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. For example, in the

event of a court subpoena requesting the case file of a client who has been receiving counselling from the counselling center.

Under these circumstances, a|CITY CHURCH will disclose requested data. However, the DIO will ensure the request is legitimate, seeking assistance from the IO, IR & the ELT as well from external legal advisers where necessary.

PROVIDING INFORMATION

A|CITY CHURCH aims to ensure that data subjects are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the church has a privacy statement, setting out how data relating to individuals is used by the church that is freely available on the church website and on request from admin@acitychurch.co.za.

POPIA POLICIES AT a|CITY CHURCH

INFORMATION SECURITY MANAGEMENT POLICY

Personal Information

This policy ensures that the organization proactively complies with all relevant privacy regulations and respects the right to privacy of data subjects.

Information classification	Information is classified according to purpose.
Documenting personal information processing activities	These are listed in the detailed Privacy Policy
Legal basis for processing activities	Processing is according to POPIA regulations
Transparency	Data subjects are informed in the following ways regarding their PI: - Details on a|CITY CHURCH policy & procedures are easily

	accessible on the church website and via email; - This includes the rights of the data subject; - Access to consent & de- consent procedures are made available on the website and via email; - Breach procedure is made clear and available on the same platforms.
Limit sharing with third parities	- a|CITY CHURCH makes no access of PI to any third parties on any level.
Personal information impact assessments	- The PAIA is the process that assists the church in identifying and minimizing the data protection risks from processing personal information. This is an ongoing process that is subject to regular re views. REF https://popia.services/popi/index.php/governancw/personal-information-impact-assessments
Records retention periods	- Records are not kept longer than is required. Duration of retention for specific PI categories are listed on the POPIA LISTING COMPLIANCE SOURCES doc . This information is included in this document.
Data subjects' rights	Data subjects are informed in the following ways regarding their PI: - Details on a|CITY CHURCH policy & procedures are easily accessible on the church website and via email; - This includes the rights of the data subject; - Access to consent & de- consent procedures are made available on the website and via email; Breach procedure is made clear and available on the same platforms.
Responsible empowered users	All users who have access to PI are required to complete a permission and confidentiality document that is submitted to the IO, RO & Senior Leader of a|CITY CHURCH. No unauthorized employees or volunteers have access to guest PI. A copy of the permission &

	confidentiality document is available on the https://bit.ly/aCITYSubjectDataRequest
Information security	The following procedures are in place to protect PI: - No unauthorized employees or volunteers have any access to PI; - No PI can be collected unless consent is given by the data subject; - All PI that appears on hard copies is prohibited from being left in a position where unauthorized personnel can gain any access. PI of this nature is to be locked in a filing cabinet if not in use; - All PI collected digitally is stored in a programme where no unauthorized personnel have any access; - Any suspected or actual breach will be reported to the IO immediately who will assess the breach, inform the RO, ELT & Senior Pastor and inform the data subject; - Impact assessments will be conducted bi- annually; - Data subjects may at any time request to see all PI that the church has stored and collected; request de- consent; - Any request to de- consent or a request to have data removed from the system will be executed witing 72 hours.
Incident management and response	a|CITY CHURCH endeavours to reduce breach incidents in so far as we are able in the following ways: - IO to regularly assess implementation of POPIA policy & procedure; - Bi- annual PI impact assessments; - Clear steps in the reporting procedures- - DIO ⇨ IO ⇨ RO ⇨ ELT (Data subject)

RECORDS MANAGEMENT

This policy ensures that the church's recordkeeping:

- Is transparent, consistent, and accountable;
- Meets legal, regulatory, and operational requirements.

HOW YOUR INFORMATION IS RETAINED

- Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—

    - retention of the record is required or authorized by law;
    - the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
    - retention of the record is required by a contract between the parties thereto; or
    - the data subject or a competent person where the data subject is a child has consented to the retention of the record.

- Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.
- A responsible party that has used a record of personal information of a data subject to decide about the data subject, must—

    - retain the record for such period as may be required or prescribed by law or a code of conduct; or
    - if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

- A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorized to retain the record in terms of subsection (1) or (2).

- The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

- The responsible party must restrict processing of personal information if—

    - its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

    - the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it must be maintained for purposes of proof;

    - the processing is unlawful, and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

    - the data subject requests to transmit the personal data into another automated processing system.

- Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

- Where processing of personal information is restricted pursuant to subsection (6), the responsible party must inform the data subject before lifting the restriction on processing.

Operational record keeping	As listed on the a|CITY CHURCH POPI INTERNAL AUDIT doc https://bit.ly/aCITYPOPI_InternalAudit
Retention schedule	As listed on the a|CITY CHURCH POPI INTERNAL AUDIT doc

	https://bit.ly/aCITYPOPI_InternalAudit
Information security	Internal measures as prescribed in the a|CITY CHURCH POPIA policy & procedures doc; Firewall (TBC)
Record management assessment	Carried out bi- annually by the DIO

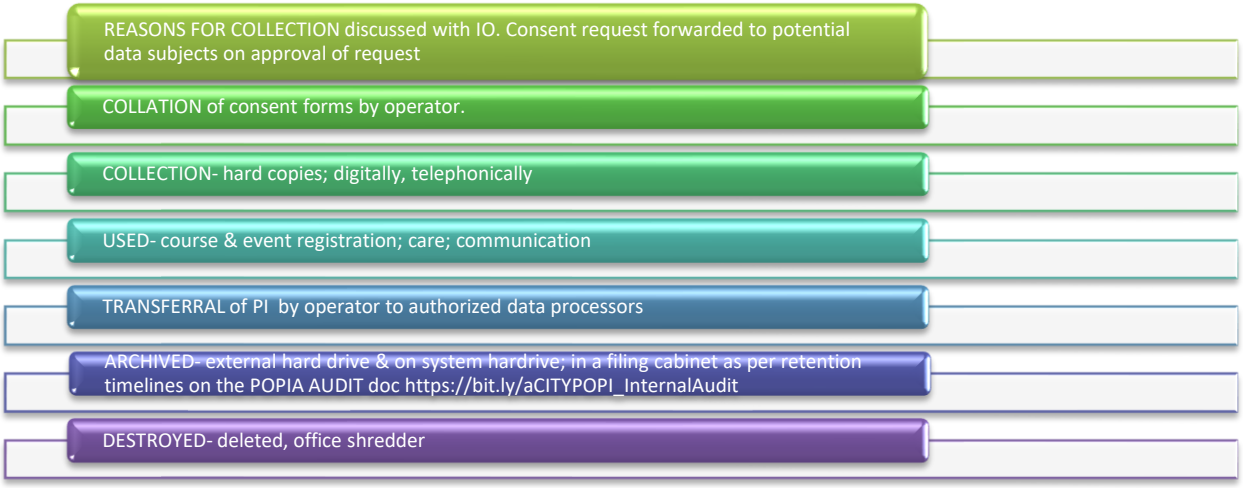
IMPLEMENTATION POLICY

Team Responsible for implementation?	IO/ DIO ELT

HOW YOUR INFORMATION IS PROTECTED

- Volunteers & staff trained to recognize personal information;
- Identify processing PROCEDURES. Check that these are complaint with the 8 Important Protection Principles as outlined by POPIA. SEE DATA LIFECYCLE that indicates how personal information is collected, used, transferred, archived, or destroyed;
- Identification of privacy risk by using the information access inventory & evaluating each area where information is accessed;
- Implement a policy & procedure to manage the risk;
- Train people to be aware of the risk and to avoid it;
- Risk response is integrated into the response plan;
- Regular policy & procedure effectiveness audit by the Information Officer

DATA LIFE CYCLE- PROCESS SUMMARY
How personal information is collected, used, transferred, archived, or destroyed.



WHAT HAPPENS IN THE EVENT OF A BREACH
BREACH PROTOCOL
According to POPIA SECTION 101, any person who contravenes the following is guilty of an offence:

A person acting on behalf or under the direction of the Regulator, must, both during or after his or her term of office or employment, treat as confidential the personal information which comes to his or her knowledge in the course of the performance of his or her official duties, except if the communication of such information is required by law or in the proper performance of his or her duties.

According to POPIA Security measures regarding information processed by an operator are as follows:

1. A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.
2. The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person.

Notification of security compromises according to SECTION 22 of the POPIA

1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the responsible party must notify—

    1.1.1 the Regulator; and
    1.1.2 subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

2. The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

3. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

4. The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

    4.1 Mailed to the data subject's last known physical or postal address;
    4.2 sent by e-mail to the data subject's last known e-mail address;
    4.3 placed in a prominent position on the website of the responsible party;
    4.4 published in the news media; or
    4.5 as may be directed by the Regulator.

5. The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

    5.1. a description of the possible consequences of the security compromise;

    5.2 a description of the measures that the responsible party intends to take or has taken to address the security compromise;

    5.3 a recommendation about the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

    5.4 if known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the personal information.

6. The Regulator may direct a responsible party to publicize, in any manner specified, the fact of any compromise to the integrity or confidentiality of

personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

REPORTING A SECURITY INCIDENT OR DATA BREACH

A "security incident" refers to any event resulting in a breach of security or unauthorized access to or acquisition, release, use, or disclosure of subject data's PI. Data breaches will typically also be security incidents, but security incidents can occur which do not involve PI. Examples of the latter could include:

- Strange or abnormal activity such as pop- ups on an office laptop;
- Any suspected or unknown authorized disclosure or use of confidential church information. For example, disclosure of confidential meeting material to unauthorized staff/ persons.

WHAT DO I DO IF I SUSPECT A BREACH?

If there is a suspicion regarding a security incident this must be reported immediately to the IO or one of the DIO's via the following methods:

- Email to admin@acitychurch.co.za;
- Completion of a SECURITY BREACH (https://forms.gle/AdpH1RgvHHepeaXF8) form on Information Central

If a person believes that the security incident may also be a data breach the same procedure as above must be followed. Failure to adhere to the protocol immediately or to provide any follow- up information that may be requested, will be treated seriously and disciplinary action may be taken.

FOLLOW- UP BREACH PROCEDURES

When a complaint is referred to the Regulator, the Regulator has certain options. He can

- conduct pre-investigation;
- act as a conciliator;
- if after investigating the complaint the Regulator believes there is no case either because of the passing of time, the trivial subject matter of the complaint, the fact that the complaint is unwarranted or not made in good faith, or if the complainant does not have a sufficient personal interest in the matter, or where there is another internal remedy which has not yet been exhausted, or where further action would be unnecessary or inappropriate, decide to take no action;
- conduct a full investigation;

- refer the complaint to the Executive Leadership Team.

The Executive Leadership Team will make recommendations regarding actions that should be taken against the responsible party.

INTERNAL MEASURES TO AVOID SECURITY INCIDENTS OF BREACH OF DATA

IT SYSTEMS ACCESS REQUIREMENTS

Only authorized devices are permitted to connect to the church systems.

Church office device connections and access considerations

- In the office only the church Wi-Fi network is to be used using available wired connections;
- When working remotely only reputable Wi-Fi sources that are known to you are to be used;
- When using internet- based applications, always try to secure an SSL connection as denoted with https:// or where you see the "closed lock" icon on your browser.

PASSWORD POLICY

Passwords and user login IDs are unique to each authorized user and may not be shared with or used by anyone other than the assigned user. The user is responsible for all activity associated with their password or user login ID.

In addition the following rules apply in relation to passwords:

- Passwords are to be kept private and will be changed every two months;
- Passwords are not to be shared or written down;
- Passwords will be saved in a centralized password vault;
- Each office laptop will have a 2FA password and thumb authentication function;
- It is prohibited to use group or shared logins;
- The IT team can reset passwords without advanced notice and use whenever there is any indication of a possible information system or password compromise;
- Staff must not email, text, or otherwise transmit your password in any unauthorized form;
- If your device requires support from the IT service provider and the support requires use of your password stay with the technician to enter your password as required; accept a temporary password change by the technician and accept a mandatory reset of your password when your device is returned.

HOW WE REQUEST USE OF YOUR INFORMATION

All forms contain a consent clause & access to the detailed Privacy Policy.

STEP ONE	All online forms that require guest info, include the following at the bottom of each page **COMMUNICATION PERMISSION** Please TICK below to ensure that we have your permission to contact you and to store your data. This will be done in accordance with the a|CITY CHURCH Privacy Policy which is complaint with the **Protection of Personal Information Act (POPI ACT),** which can be viewed here: https://bit.ly/aCITY_Policy I give a|CITY CHURCH permission to contact me via email, WhatsApp or with a call from the church admin office with regards to my request. ○ Yes ○ No
STEP TWO	**a|CITY CHURCH PRIVACY POLICY** a|CITY CHURCH uses personal data of individuals for the purpose of general church communication & administration. a|CITY CHURCH recognizes the importance of the correct & lawful handling of personal data. All personal data, whether it is kept on paper, computer, or other media, will be subject to the appropriate legal safeguards as specified in the POPI ACT 2020. (Protection of Personal Information Act) a|CITY CHURCH fully endorses and adheres to the eight principles of the POPIA. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport, and store personal data for a|CITY CHURCH must adhere to these principles. **THE PRINCIPLES** The principles require that personal data shall be managed in accordance with stipulations as listed: 1. **Accountability. :** a|CITY CHURCH has designated a "Responsible Person" to give effect to the POPI principles below and to ensure that the principles set out and all the measures that give effect to the principles are complied with. 2. **Process limitations**

Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of any individual. Personal information may only be processed for the purpose it was intended for, provided that the information is relevant and not excessive. Personal information must be collected directly from the persons concerned when they come to church or any of its outreach programme.

3. **Purpose specifications**. Personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the church. It is imperative that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently used. In terms of membership or where minors need to be signed in for security reasons, people need to consent to the retention of the records.

4. **Further processing limitations**. a|CITY CHURCH'S "Responsible Person" will always consider the following; (a) make sure that the person concerned has given consent to process their information, (b) whether the member has not requested deletion prior to processing their information and (c) whether the information is compatible with the purpose of collection, available in a public record.

5. **Quality of information**. The church's "Responsible Person" will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary for the purpose it is intended.

6. **Openness**. Personal information collected as part of membership or any transaction will include a name, address or contact detail such as an email address. This is collected in a fair and transparent manner. To ensure that the processing of information is fair, individuals will be aware of what specific personal information is being held by the church. a|CITY CHURCH will 'register' by submitting a notification to the Regulator before commencing

the processing of personal information.

7. **Security safeguards**. a|CITY CHURCH through the "Responsible Person" will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organizational measures. Appropriate internal control measures are in place and regularly evaluated i.e., ensuring that security practices and procedures are effective and in place. All employees and volunteers processing personal information on behalf of the church will always, (a) process this information with the knowledge or authorization of the church; and (b) treat personal information which comes to their knowledge as confidential and will not disclose it. Should there be a breach the church will notify the Information Regulator and the data subject as soon as it practically possible. The church will consider the legitimate needs of law enforcement or any another reasonable measures to determine the scope of the breach to the data subject and to restore the integrity of the church. A notification providing sufficient information to allow the affected person/s to take protective measures against the potential consequences of the compromise, including, if known to the church, the identity of the unauthorized person who may have accessed or acquired the personal information will be provided to the data subject concerned.

8. **Personal information on record & third-party disclosures.** The church must make provision for the members, who have provided adequate proof of identity, to request what personal information the church holds about them, including third parties the church may have shared the member's personal information with.

HOW WE COLLECT DATA & INFORMATION ABOUT YOU

We collect personal information each time you are in contact with us. For example, when you:

- Visit our website;
- Book for an in- person service;
- Register for an event;
- Responsible, empowered users Complete any of the online forms;

- Communicate with the Church Clear roles and responsibilities in the implementation of the policy by email;
- Receive counselling;
- Access to social media platforms such as Facebook, YouTube, WhatsApp, Instagram.

MAINTAINING CONFIDENTIALITY

a|CITY CHURCH will treat all your personal information as private and confidential and will not disclose any data about you to anyone other than the leadership and operational team leaders of the church to facilitate administration and day- to-s day ministry of the Church.

All a|CITY CHURCH staff & volunteers who have access to Personal Data will be required to agree to sign a Data Protection Policy.

There are four exceptional circumstances to the above:

1. Where we are legally compelled to do so;
2. Where there is a duty to the public to disclose information;
3. Where the disclosure is to protect your interests;
4. Where the disclosure is made at your request or with your consent.

USE OF PERSONAL INFORMATION

- The day-to-day administration of the church. For example, ACC calls, preparation of service run sheets, notification of team leader days.
- Contacting you to keep you informed about small groups, church events, services, and activities.
- Executive reports that require the collation of statistics. For example, church attendance, small group attendance.

The Database (Anatomy)

This database can only be accessed by staff and volunteers who have been authorized to do so by the Senior Leaders.

- Access is controlled using a login username;
- Only Senior Leaders have access to all information on the database. All other authorized staff & volunteers have limited access to specific sections.
- Staff & volunteers who have access are the church administrator and members of the ACC team (a|CITY Care Team).
- None of your information is passed on to third parties outside the church environment without your consent.
- Sensitive, personal information is kept strictly confidential. It is never sold, given away or otherwise shared with anyone, unless required by law.

RIGHTS TO ACCESS INFORMATION

Employees and other subjects of personal data held by a|CITY CHURCH have the right to access any personal data that is being held in certain manual filing systems. This right is subject to certain exemptions: Personal

Information may be withheld if the information relates to another individual.

Any person who wishes to exercise this right should make the request in writing to the a|CITY CHURCH Information Officer admin@acitychurch.co.za

If personal details are inaccurate, they can be amended upon request.

a|CITY CHURCH claims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days of receipt of a completed form https://bit.ly/aCITYSubjectDataRequest unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

TYPE OF INFORMATION WE COLLECT

a|CITY CHURCH has a Personal Information Inventory that lists all the areas where the following information is required from guests; volunteers & staff

- Demographic information;
- Contact information;
- Preferences;
- Background information

  This inventory includes special personal information that requires extra care
- Client information obtained during counselling.

YOUR RIGHTS & CHOICES

- Everyone has the right to privacy;
- The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information;
- You have a right to privacy regarding the collection, use and storage of your personal information. This includes the right to de- consent to the collection of your personal information by the church and the right to decline the provision of your personal information;
- a|CITY CHURCH has consent options regarding the collection of personal information on all forms & areas where any kind of personal information is required from you;
- Attached to all of these consent options are details regarding our privacy policy that include how the data is collected, what it is intended for and the like;
- You have the right to de- consent or to decline consent. There are notification links that assist you in requesting these

https://bit.ly/aCITYSubjectDataRequest Your information will be deleted within 72 hours of your request. Any hard copies of information requested from you will be shredded by the operator. A report of the de- consent will be noted by the Information Regulator.

CHILDREN CONSENT FORMS FROM GUARDIANS

- Personal information may only be processed if—the data subject or a competent person where the data subject is a child consents to the processing.

RETENTION OF DATA

- a|CITY CHURCH will retain your personal information for only as long as is necessary for the purposes as set out in this policy.

CHANGES TO OUR PRIVACY POLICY

- a|CITY CHURCH reserves the right to change the Privacy Policy at any time. When this policy is revised, we will post the updated version on our website and send a notification to all registered data subjects. Your continued use of our site indicates your acceptance of these changes.

SMS/ WHATSAPP PRIVACY POLICY

- We respect your privacy and will not distribute your mobile contact details to any third parties;
- If at any time you need our contact information on how to discontinue text messages, please send HELP to admin@acitychurch.co.za. We will then delete your mobile number from our storage database;
- By subscribing, you have provided us with consent to send you text messages regarding our church's events and updates. Message frequency varies by events;
- In general, the messages we send provide you with information about our church events. Some of the text messages we send may include links to websites. To access these websites, you will need a web browser and internet access.

DIRECT MARKETING

All direct marketing is ring- fenced to only existing clients or new clients who have expressly consented to further marketing. The data subject must also have an option to opt-out or unsubscribe from any form of direct marketing. Therefore we will be sending out a communication to all clients on the existing database to confirm that the company is now POPI complaint and that any individual can opt- out of further marketing material.

We sent out a newsletter/ electronic consent form to all existing members to

	reaffirm the church's undertaking to continue to process any personal information in its possession lawfully and securely in terms of POPI Should you have any queries or concerns regarding the above, please contact the Church office admin@acitychurch.co.za

Should you have any queries or concerns regarding the above, please contact the Church office
admin@acitychurch.co.za

APPENDIX

Please note that digital forms are accessible via links provided in the a|CITY CHURCH POPI Policy & Procedures doc

PERMISSION & CONFIDENTIALITY FORMS

FORM A
OPERATOR PERMISSION & CONFIDENTIALITY FORM

OPERATOR. This is a person who captures data subject personal information on behalf of a|CITY CHURCH once the data subject has given consent for this to take place.

My position at a|CITY CHURCH.
Please tick

○ Employee

○ ACC (a|CITY CHURCH CARE) volunteer

○ OTL (Operational Team Leader)

○ Other
Please specify _____

Reason for permission request:
Please tick

○ I need to collect subject data to store on the a|CITY CHURCH data base system;

○ I am an ACC member I need to use subject data for pastoral care purposes;

○ I need contact data subjects to confirm registrations; bookings; meetings & to provide information pertaining to these;

○ I need to process data subject consent & de- consent requests

I, _____ (Name & surname) have read through the a|CITY CHURCH POPIA. I accept and will comply with the terms and conditions as stipulated in this policy.

a|CITY CHURCH POPIA Policy & Procedures https://bit.ly/aCITY_Policy

_____ _____
Signed Date

FOR OFFICE USE ONLY
Date application received: _____
Date application was processed: _____

○ Application approved;

○ Application denied

_____ _____
Date Signed

FORM B

SUBJECT DATA CONSENT FORM

I _____ (Name & surname) hereby give consent for personal information to be collected, processed, and stored by a|CITY CHURCH. I have read through the a|CITY CHURCH POPIA Policy and procedures document. I know my rights and accept the terms & conditions in this document.

a|CITY CHURCH POPIA Policy & Procedures https://bit.ly/aCITY_Policy

_____

_____

Date Signed

FORM C

SUBJECT DATA DE- CONSENT/ REQUEST FOR DATA UPDATE/ REQUEST FOR DATA TO BE REMOVED FORM

I _____ (Name & surname) hereby request:

- ○ That all personal information pertaining to me be removed from a|CITY CHURCH data collection platforms;
- ○ That consent to collect, store & process my personal information be revoked;
- ○ To update my personal information. Please specify information that has changed & provide the updated information

  Name _____

  Mobile _____

  Email _____

  Address_____

  Other. Please specify _____

  _____

I have read through the a|CITY CHURCH POPIA Policy and procedures document. I know my rights and accept the terms & conditions in this document.

a|CITY CHURCH POPIA Policy & Procedures https://bit.ly/aCITY_Policy

_____

_____

Date Signed

FORM D

APPOINTMENT LETTER FOR INFORMATION OFFICER ROLE: a|CITY CHURCH

The Information Officer role is by default that of the Designated Head of a Private Body in terms of the provisions of both the Promotion of Access to Information Act 2 of 2000 (PAIA) and the Promotion of Personal Information Act 4 of 2013 (POPI). The responsibilities defined for these roles in Urban Edge Church (registration number:), a private body in terms of the aforementioned Acts are:

1) **POPI Act Section 55 (1): An Information Officer's responsibilities include:**

a) the encouragement of compliance, by the body, with the conditions for the lawfulprocessing of personal information;
b) dealing with requests made to the body pursuant to this Act;
c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 (prior authorization) in relation to the body;
d) otherwise ensuring compliance by the body with the provisions of this Act; and
e) as may be prescribed.

POPI Regulations 2018: Responsibilities of Information Officers

2) **Regulation 4:**

a) An Information Officer must, in addition to the responsibilities referred to in s55(1) of the POPI Act, ensure that:

i) A compliance framework is developed, implemented, monitored, and maintained; ii) A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

iii) A manual is developed, monitored, maintained, and made available as prescribed in s14 and s51 of the PAIA Act;

iv) Internal measures are developed together with adequate systems to process requests for information or access thereto; and

v) Internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

b) The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

POPI Act: Section 56: Designation and delegation of deputy Information Officer(s)

3) Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of –

a) Such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and

b) Any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

a|CITY CHURCH Information Officer role appointment acceptance:

Signature:
D.A. Sloane

Date of Appointment Acceptance: July 2021

a|CITY CHURCH Deputy Information Officer role appointment acceptance:

Signature:
F.Erispe
Date of Appointment Acceptance: July 2021

Signature
C.Delport
Date of Appointment Acceptance: July 2021

FORM E

REPORTING A SECURITY BREACH FORM

https://forms.gle/AdpH1RgvHHepeaXF8

FORM F

REQUEST TO USE PHOTOGRAPHS/ VISUAL RECORDINGS

a|CITY CHURCH is fully complaint with the provisions of the Protection of Personal Information Act 4 of 2013 ("POPI"), where applicable. For more information relating to a|CITY CHURCH, or any of its associated divisions, privacy policy, please visit the a|CITY CHURCH website www.acitychurch.co.za or https://bit.ly/aCITY_Policy

a|CITY CHURCH would like to request the use of the following:

- ○ Photograph of you;
- ○ Video clip where you are the speaker
- ○ Group photo of which you are a part

PURPOSE. Use on one of the a|CITY CHURCH social media pages for the following. All of which are related to a|CITY CHURCH:

- ○ To promote an upcoming event/ programme ;
- ○ As a devotion
- ○ As a personal testimony
- ○ To showcase a service/ event that has already taken place

I, _____ (Name, surname)

- ○ Consent
- ○ Reject

The request to use photographs/ clips where I am visible.

Thank you. Please return this form to admin@acitychurch.co.za

FINANCIAL SERVICE PROVIDER

STANDARD BANK

https://www.google.com/search?q=standard+bank+terms+and+conditions&oq=STANDARD+BANK+TERMS+AND+CONDITIONS&aqs=chrome.0.0l2j0i22i30l8.11928j0j15&sourceid=chrome&ie=UTF-8#

GENERAL SERVICE PROVIDERS

Quicket Privacy Policy

https://help.quicket.com/portal/en/kb/articles/privacy-policy

Anatomy Privacy Policy

https://release.anatomy.org.za/anatomy/privacypolicy.htm

SARS Privacy Policy
https://www.sars.gov.za/privacy-policy/

Xneelo Privacy Policy
https://xneelo.co.za/legal/privacy-policy/

HOW WE PROCESS YOUR PERSONAL INFORMATION

DREAM TEAM
COVID SCREENING FORMS/ REGISTRATION LISTS
CONTENT
Name;
Surname;
Cell;
Temp;
Tested for COVID/ had COVID?

NEXT
Hard copies & excel spreadsheets stored for two weeks in a file in a filing cabinet in a locked office.

ADMIN
QUICKET REGISTRATION
CONTENT
Name;
Surname;
Email address;
Cell number;
Suburb;
First time guest;
Returning guest;
Age of child/ren

NEXT
Quicket, spreadsheet which has 3 columns for adults, kids, and PULSE. Info is forwarded onto WhatsApp group. Deleted one week later.

KIDS/TOTS/PULSE
COVID SCREENING FORMS
CONTENT
Name;
Surname;
Temp;
Tested for Covid;

Had Covid;

NEXT

Hard copies stored for two weeks and shredded

ADMIN
DAILY SCREENING FOR PEOPLE ENTERING THE CAMPUS
CONTENT
Name;
Surname;
Cell number;
Have you tested for COVID;
Has anyone in your household tested positive;

NEXT
Hard copies stored for two weeks and shredded

ADMIN/ NEW PEOPLE/ACC
FIRST & SECOND TIME GUESTS
CONTENT
Name;
Surname;
Email;
Cell number;
Age;
Life stage;

NEXT
Guest info forwarded to ACC by operator. Contact made on a Thursday. Guest info kept on record. Annual update all guests who no longer attend the church are deleted off the system. Guests who still attend are asked to update details once a year.
APPLICATION FOR MEMBERSHIP
CONTENT
Name;
Surname;
Email;
Cell number;
Age;
Life stage;

NEXT
Application is submitted to the lead pastor. If the applicant is successful the outcome of the application is communicated via email. The information is captured onto a central membership data base excel spreadsheet. If a hard copy was submitted it is kept in a filing cabinet in a locked office

ACC

NEW BELIEVER/RE-COMMITTEMENT/FIRST & SECOND TIME GUESTS/PASTORAL CONTENT

Name;
Surname;
Email;
Cell number;
Age;
Life stage;
What the person needs assistance with which would indicate personal need, for example, needs food, is unemployed, needs counselling, needs prayer.

NEXT

Shred hard copies. Information is captured onto a central data base and is stored for 5 years.

ADMIN

BABY BLESSING

CONTENT

Name;
Surname;
Email;
Cell number;
Child/ren's name/s;
Age/s

NEXT

Shred hard copies after event. Information is captured onto a central data base and is stored for 5 years.

BELIEVER'S BAPTISM

CONTENT

Name;
Surname;
Email;
Cell number;

NEXT

Shred hard copies. Information is stored on a central data base and is stored for 5 years.

COUNSELLING

CLIENTS

CONTENT

Name;
Surname;
Email;
Cell number;
Address;
Member of the church or not;
Name and surname of person who referred the client

NEXT
Hard copies- in storage in lead pastor's locked office- 10 years. Digital storage. Microsoft office. Lead pastor's laptop.

MARRIAGE OFFICER
COUPLES
CONTENT
Name;
Surname;
Address;
Qualification;
Employment;
ID;
Cell – couple;
Name, surname, cell - Witness

NEXT
Couple emails request to be married. Staff member responds with blank application forms that are completed and returned via email. Hard copies- in storage in lead pastor's locked office- 10 years. Copies from the marriage register as per legal requirements are submitted to the Department of Home Affairs 3 days after the solemnization of the marriage by the church marriage officer. A copy is left in the marriage register & a copy is handed to the couple. The marriage register is submitted to Home Affairs once it is full. The department then keeps the full register in their vault.

ACC TEAM
PRAYER REQUESTS & PRAISE REPORTS
CONTENT
First name;
Surname;
Email;
Cell number;
Member of the church;
Life stage;
Sometimes medical; marital, details based on the needs

NEXT
Subject data on the card & on INFO CENTRAL is transferred onto Anatomy. The card is shredded once the data has been captured. The data on INFO CENTRAL is stored for one year and then deleted.

HEART PAGE (Website)
REQUEST FOR PRAYER
CONTENT
First name;
Surname;
Email;
Cell number;

Member of the church;
Life stage;
Sometimes medical; marital, details based on the needs

NEXT
Subject data on the card & on INFO CENTRAL is transferred onto Anatomy. The card is shredded once the data has been captured. The data on INFO CENTRAL is stored for one year and then deleted.

REQUEST FOR COUNSELLING
CONTENT
First name;
Surname;
Email;
Cell number;
Attend the church;
Life stage;
Age;
Sometimes personal details pertaining to employment, health, relationship issues dependent on the type of praise report.
Clients also complete a consent form regarding confidentiality as well as CPSC (Council for Pastoral & Spiritual Counsellors) consent & indemnity agreement.

NEXT
WhatsApp & email. Keep numbers as long as they are in counselling. Then delete. If counselling resumes, new request made & info stored on the administration phone. All counselling notes are kept in a locked filing cabinet in a locked office for 10 years.

REQUEST FOR FOOD PARCEL
CONTENT
First name;
Surname;
Email;
Cell number;
Attend the church;
Life stage;
Age;
Sometimes personal details pertaining to employment, health, relationship issues dependent on the type of praise report.

NEXT
Spreadsheet. Office. Guests receiving parcels. Keep for a year once parcel distribution is no longer required per guest.

REQUEST FOR EMPLOYMENT
CONTENT
First name;
Surname;
Email;
Cell number;

Attend the church;
Life stage;
Age;
Sometimes personal details pertaining to employment, health, relationship issues dependent on the type of praise report.

NEXT
Data subject information deleted after one month

ADMIN
GROW TRACK SIGN UP/JOIN A SMALL GROUP/BECOME A SMALL GROUP LEADER/SHORT COURSES/PATHWAY REGISTRATION
CONTENT
First name;
Surname;
Email;
Cell number;
Attend the church;
Life stage;

NEXT
Grow Track - New Peoples list. Annual internal audit. Delete.
Small Group - Delete info at the end of each 12-week module. Reapply.
BECOME A SG LEADER - If lead per module. Delete. Re- apply
SHORT COURSES - Information deleted post event.

ADMIN/FINANCE
STAFF DETAILS
CONTENT
First name;
Surname;
Address;
Cell;
ID;
Tax number

NEXT
Retained for 5 years in locked filing cabinet in a locked office.
PAY SLIPS
Name;
Surname;
Income;
UIF;
PAYE;
Employee tax;
Medical aid

NEXT

Retained for 5 years in a locked filing cabinet in a locked office.

PAYROLL MONTH ANALYSIS

CONTENT

Name;
Surname;
Gross;
Nett;
PAYE;
UIF;
Leave accrual

NEXT

Retained for 5 years in a locked office in a locked filing cabinet.

UIF

CONTENT

Name;
Surname;
ID;
UIF portion paid pm

NEXT

Retained for 5 years in a locked filing cabinet in a locked office.

EMP 201

CONTENT

Name;
Surname;
Amount payable;
PAYE;
UIF

NEXT

Retained for 5 years in a locked filing cabinet in a locked office.

LEAVE HISTORY

CONTENT

Name;
Surname;
Leave accrual

NEXT

Retained for 5 years in a locked filing cabinet in a locked office.

PERIODIC SCHEDULE

CONTENT

Name;
Surname;
Basic salary;
UIF;

PAYE;
Gross;
Nett

NEXT
Retained for 5 years in a locked filing cabinet in a locked office.

PAYMENT FILE
CONTENT
Name;
Surname;
Nett
NEXT
Retained for 5 years in a locked filing cabinet in a locked office.

BANK TRF LIST
CONTENT
Name;
Surname;
UIF/PAYE amount

NEXT
Retained for 5 years in a locked filing cabinet in a locked office.

ADMIN
STAFF PERSONAL FILES THAT CONTAIN: LEAVE FORMS, STAFF APPRAISALS, CONTRACTS, DISCIPLINARY MATTERS, SALARY INCREASES, COPY OF ID
CONTENT
Name;
Surname;
Mobile;
DOB;
ID;
Postal address;
Physical address;
Marital status;
Spouse name;
email address;
banking details;
tax number;
race

NEXT
Retained for 5 years in a locked filing cabinet in a locked office.

ADMIN/OFFERING
GIVING ENVELOPES/CREDIT CARD ONLINE GIVING
CONTENT

Name;
Surname;
Card number;
Phone;
Email;
Delivery address

NEXT
Shredded once cash has been removed.

EVENTS
CHURCH EVENTS
CONTENT
Name;
Surname;
Email;
Cell number;
Dietary requirements

NEXT
Kept and filed with source doc. Once attendance numbers and income tally- form shredded. Info Central. Post event GOOGLE sheet deleted.

OPERATIONAL LEADERSHIP TEAMS
OLT, TD, RADIANT, SG LEADERS, KIDS LEADERS, WAVE, PULSE, TOTS, KIDS TEAM - VOLUNTEERS, DREAM TEAM, PRODUCTION, BAND, SG ATTENDEE GROUPS, FINANCE TEAM, EXECUTIVE LEADERSHIP TEAM, KIDS TEAM – PARENTS, TOTS – PARENTS, ACC, STAFF WHATSAPP
CONTENT
Name;
Surname;
Cell number

NEXT
Once groups are no longer functional, the group administrator will delete each participant and then delete the group. This applies to all church WhatsApp groups.

SOCIAL JUSTICE – STITCH2STITCH
INTERVIEW FORM
CONTENT
First name;
Surname;
Cell;
Address;
employment history;
education history;
current medication;
ID number;

courses studied;
additional education;
interview notes made by interviewer;
medication currently taking;
name, surname and age of children;
marital status

NEXT
Hard copies kept in a locked filing cabinet in a locked office. All information is kept for a period of 5 years once trainee has completed the programme.

A|CITY CONNECT
JOB APLLICATION/ADVERTISING EMPLOYMENT PSOITIONS/ADVERTISING BUSINESSES
CONTENT
Name;
Surname;
Cell number;
Address;
Marital status

NEXT
Job app forms & Advertising employment - PI is deleted after 3 months. All posts are removed from the site after 3 months. This includes PI as provided by the subject
Advertising businesses - All posts are removed from the site after 3 months. This includes PI as provided by the subject