



**CONNEXIONS**

011 849 6012

info@connexionschurch.co.za

www.connexionschurch.co.za

# Connexions Church

Data Protection Policy & Procedure

July 2021

Authorised: Name

Gwen Bennett

Signature: \_\_\_\_\_

G/S

Any questions relating to the contents of this document can be relayed to the above authorized person and / or  
info@connexionschurch.co.za



## Contents

### INTRODUCTION

1. Why this policy is important.
2. How this policy applies to you and what you need to know
3. HR & Internal data collected, stored and processed.
4. Website, Cookies & Marketing
5. Cybersecurity & Data Breach Protection

### POLICY AND PROCEDURES

Finance  
Motion Track  
Hosting & Hospitality  
Connect Groups  
Funerals  
Pastoral  
Courses & Events  
Worship & Production  
Young Adults Connect  
Reception  
Connect Youth  
WordPress  
Anatomy database  
Kids Connect  
IT  
Communication

### FINANCIAL SERVICE PROVIDERS

1. First National Bank
2. YOCO
3. Snapscan

### GENERAL SERVICE PROVIDERS

1. Wordpress Privacy Policy
2. Anatomy Privacy Policy
3. SARS Privacy Policy
4. Investec Privacy Policy
5. Ricoh Privacy Policy
6. Sage Privacy Policy
7. Afrihost Privacy Policy
8. Finsure Privacy Policy
9. Liberty Privacy Policy
10. CMS Privacy Policy



11. Dropbox Privacy Policy
12. Google Drive Privacy Policy
13. Apple ID Privacy Policy

## CONNEXIONS CHURCH COMPLIANCE

### INTRODUCTION

Connexions Church is committed to protecting personal data and respecting the rights of our data subjects (People whose personal data we collect and use). Connexions Church values the personal information entrusted to us and we respect that trust by complying with all relevant laws\* and adopting good practice.

(\*Protection of Personal Information Act, hereinafter "POPIA")

We process personal data to help us:

- Maintain a database of our church partners.
- Provide pastoral support for partners and others connected with our church.
- Provide services to the community.
- Safeguard children, young people, and adults at risk
- Recruit, support and manage staff and volunteers.
- Maintain our church accounts and records.
- Promote our services.
- Maintain the security of property and premises.
- Respond effectively to enquirers and handle any complaints.
- For any fundraising events that might require this information

This policy has been approved by the Connexions Church Leadership Team who are responsible for ensuring we comply with our legal obligations. It sets out the legal rules that apply whenever we gather, process, store or use personal data.

#### 1. Why this policy is important

A. We are committed to protecting personal data from being misused, getting into the wrong hands because of poor security or being shared carelessly, or being inaccurate.

B. This policy sets out the measures we are committed to taking as a church and what each of us will do to ensure we comply with the relevant legislation.

For instance, we will make sure that all personal data is:

- \* Processed lawfully, fairly and done transparently.
- \* Processed for specific and legitimate purposes and not in a manner that is incompatible with those purposes.



- \* Adequate, relevant, and limited to what is necessary for the purposes of which it is being processed.
- \* Accurate, complete, and up to date
- \* Not kept longer than necessary for the purposes for which it is being processed.
- \* Processed in a secure manner, by using appropriate technical and organizational means.
- \* Processed in keeping with the rights of data subjects regarding their personal data.

## 2. How this policy applies to you and what you need to know

A. As an employee, volunteer, or trustee processing personal information on behalf of the church, you are required to comply with this policy. If you think that you have accidentally breached the policy, it is important that you contact our Information Officer immediately so that we can take action, try to and limit the impact of the breach. Anyone who breached the policy intentionally, recklessly or for personal benefit they may also be liable for prosecution or to regulatory action.

B. As a leader and/or manager you are required to make sure that any procedures that involve personal data, which you are responsible for in your area, follow the rules set out in this Data Protection Policy.

C. As a data subject of Connexions Church, you can be assured that we will handle your personal information in line with this policy.

D. As an appointed data processor/contractor, you are required to comply with this policy under the contract with us. Any breach of this policy will be taken seriously and could lead to us taking contract enforcement action against the company or terminating the contract.

E. Our Information Officer is responsible for advising Connexions Church and its staff and members about their legal obligations under data protection law, monitoring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about this policy or any concerns that the policy has not been followed should be referred to them at [info@connexionschurch.co.za](mailto:info@connexionschurch.co.za).

Before you collect or handle any personal data as part of your work (Paid or otherwise) for Connexions Church, it is important that you take time to read this policy carefully and understand exactly what is required of you, as well as the organization's responsibilities when we process data.

## 3. HR & Internal data collected, stored and processed

A. Employees and staff are periodically trained on what is lawful processing of personal information and the risks associated with day-to-day handling and processing of personal information should be addressed and limited through education.



B. A clause has been added to each employment contract to confirm the company's undertaking to ensure that the employee's personal data will be securely held and lawfully processed in terms of POPI (data protection clause).

C. Connexions Church uses Google Drive for its online solutions. Google drive provides decent cybersecurity and levels of encryption, which allows for secure and accountable processing of personal data. Furthermore, it allows for creating back-ups and can be used to create a hybrid cloud for the company. Permissions and access should remain controlled and limited to the different departments. Any breach of personal data will be reported to the Regulator and all efforts must be taken to contain the breach. Thereafter, data subjects will be informed of the extent of the breach.

#### **4. Website, Cookies & Marketing**

A. We believe that transparency is important when dealing with data subjects and their personal information, therefore our website collects limited personal information but is still compliant with POPIA. We therefore have an Online Privacy Policy and have added the attached email disclaimer to every employee's email signature.

B. The Online Privacy Statement includes what data is collected and processed by the Company by any data subjects who visit the website. This information includes but is not limited to contact details, email address, cookies, and in some cases, financial information (for donations of payment being made via the website).

C. The 'Connexions Church POPIA: Policies and Procedures' document is available on the website for data subjects to peruse should they need to know how their data is being processed within each department and by each service provider of the church. For added information we have included the letter of appointment for its Information Officer (head of the organization or company) and a Deputy Information Officer (someone within the organization or Company who will fulfill the role and/or attend to the duties – usually Admin or Finance Staff).

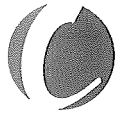
D. All direct marketing is ring-fenced to only existing clients or new clients who have expressly consented to further marketing. The data subject must also have an opt-out or unsubscribe from any form of direct marketing. Therefore, we will be sending out a communication to all clients on the existing database and confirm that the company is now POPIA compliant and that any individual can opt-out of further marketing material (pop-up or clickable box).

E. 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 POPIA.

#### **5. Cybersecurity & Data Breach Protection**

A. Google Drive, One Drive and Dropbox used by Connexions Church provides secure data protection and storage. The privacy Policies are easily accessible and are compliant with GDPR and POPIA provisions.

B. Furthermore, Google Drive, One Drive and Dropbox allows Connexions Church to create a hybrid compliant cloud system which includes comprehensive, multi-layered protection.



C. Any further processing of the personal data under Connexions Church's control is done in terms of data transfer or data-sharing agreement, which agreement is in terms of POPIA, and the action has been consented to by the data subject prior to further processing (for any reason outside of the scope for which the personal data was collected for).

D. All personal data collected, stored and processed by Connexions Church is done within a POPIA compliant framework – accompanied by the necessary consent from all members, visitors or staff (to have their data processed).

E. Please note that as Connexions Church deals with a lot of personal information, including medical conditions and certain preferences or conditions. We ensure that our internal practices are backed up by written policy or secure procedure which promotes secure and lawful processing of personal information, at all times.

## POLICY & PROCEDURE

### Finance

1. Vendor / Supplier Invoices
  - 1.1 Staff member receives invoice and hands it in to the Finance office.
  - 1.2 Staff member hands in a payment requisition with the attached invoice.
  - 1.3 Papers are kept in the employee's desk tray until scanned and emailed to the Finance Officer.
  - 1.4 Paper trail is discarded.
  - 1.5 All paid invoices with paperwork are filed electronically in the specified campus One Drive Finance File which is password protected.
  - 1.6 The Finance office is off site.
2. All HR/employee contracts/pension information forms etc.
  - 2.1 These are stored electronically in Google Drive.
  - 2.2 Any employee information / banking details/ pension forms etc. sent on email are stored on a computer which is password protected.
  - 2.3 The HR office is off site.
  - 2.4 Staff reimbursement forms / staff fuel claim
    - 2.4.1 Staff member submits payment reimbursement /claim via email.
    - 2.4.2 The email is kept in the Finance office in box until processed/paid.
    - 2.4.3 All paid claims are filed electronically in a password protected online file.
3. Financial documents / records from previous years (up to 5 years)
  - 3.1 These are stored electronically in a password protected online folder.

### Motion Track

1. A disclaimer is present on all Motion Track cards and online forms.
2. GROW Track/Becoming/Devoted Follower
  - 2.1 The guest's complete registration/screening/partnership forms which are collected by the course facilitator and handed directly to the database administrator.
  - 2.2 Forms are dropped in the safe. Finance staff opens the safe door on a Monday morning and hands the forms to the Administrator.



- 2.3 The Administrator processes all the information on Monday morning, adding all the information to the Anatomy database.
- 2.4 All sign-ups for the courses are filed for a period of 6 months, this file is stored in a locked cupboard. Documents are scanned and saved on an external drive which is kept in the safe.
- 2.5 All registration and screening forms are put in an envelope with connect cards and stored in locked in a cupboard in the office.
- 2.6 After 3 months, forms are shredded.
3. Connect Cards
  - 3.1 People drop Guest Response cards in a container at the Info desk or Guest lounge at the end of the service on exiting the sanctuary. These two places are manned with a volunteer. The cards include visitor, salvation, child blessing, baptism, connect group and serve sign ups.
  - 3.2 Volunteers put all the cards, from the designated drop off areas, into the safe.
  - 3.3 The Finance staff member opens the safe on Monday and give the cards to the Administrator.
  - 3.4 The Administrator receives the cards and processes all the information.
  - 3.5 The Administrator will process the information immediately and if not, will lock the cards away until it can be processed.
4. Guests and Salvations
  - 4.1 People fill in a Guest Response Card from the sanctuary or Guest Lounge and follows the process for Guest Response Cards.
  - 4.2 The Administrator sends an email and adds them to the Contacts list on anatomy
  - 4.3 A short welcome message is sent to the new guest, on a Monday to welcome the new guest. Requesting them to save the Church number, the message includes a POPIA disclaimer to opt in or out to retain their information or not. The new guest's information will only be saved on the Church phone if the guests confirm their Opt in permission.
  - 4.4 The card is kept for 3 months, then scanned and saved on an external drive, and then destroyed.
5. Child Blessing
  - 5.1 People sign up via an online form on the website (they need to give permission for us to use their information) information gets emailed to the Administrator, whose computer is password protected.
  - 5.2 The Administrator adds the information to an Excel spreadsheet and contacts the people who have signed up.
  - 5.3 The spreadsheet gets used by the Administrator to prepare the runsheet and is emailed to the Media staff member for the Sunday slides.
  - 5.4 The spreadsheet gets printed and put out at the info desk on the Sunday morning to register the family.
  - 5.5 The spreadsheet information is updated on the Anatomy database, by the administrator. The spreadsheet is destroyed.
6. Baptism



- 6.1 People sign up by registering via an online form on the website (they need to give permission for us to use their information) information gets emailed to the Administrator, whose computer is password protected, or they can sign up during their attendance at GROW Track.
- 6.2 The process for GROW Track above is followed.
- 6.3 The Administrator adds the information to an Excel spreadsheet and contacts the people who have signed up.
- 6.4 The spreadsheet gets used by the Administrator to prepare the runsheet and is emailed to the Media staff member for the Sunday slides.
- 6.5 Once the person gets baptized, that form is returned to the Administrator.
- 6.6 The Administrator updates each persons' profile on Anatomy (protected by the fire wall).
- 6.7 The sign-up form and spreadsheet must be destroyed.
7. Open House Event
  - 7.1 The event registration takes place via the website.
  - 7.2 The Administrator prints the registration list for check in on the night.
  - 7.3 The list is destroyed after the event.
8. Dream Team sign ups
  - 8.1 Option to sign up via GROW Track – Follow GROW Track process.
  - 8.2 Option to sign up via Connect Card – Follow the Connect Card process.
  - 8.3 Option to sign up via the website – Disclaimer is in place.
  - 8.4 Each person's details are then added to Anatomy to create an online follow up for the relevant person.

## Hosting & Hospitality

1. Giving envelopes are placed at the back of the seats for the congregation.
2. People who choose to, then personally and willingly put on their personal information on the envelope (if applicable).
3. During an allocated time in the service, every person who chooses too, places their envelope into a collection bucket which is taken around by a volunteer.
4. All the buckets are collected and given to the team leader and one other, unrelated team member. They take the buckets with its contents to the Administration office.
5. They transfer the contents into an offering bag and lock it away in the safe.
6. The offering bags are then collected from the safe by the Finance staff/Team leader.
7. Any money contained in the envelopes are counted by the Team leader and an allocated, and vetted, team member (the room in which counting takes place has a camera and a locked door). Once the counting is complete, envelopes are ripped up and thrown away.
8. Covid Screening forms / Registration lists
  - 8.1 People register and acknowledge the disclaimer willingly via the website registration link or in person. They willingly provide their personal details during this process.
  - 8.2 The Administrator prints the registration list from the online registration platform on the morning of the service.
  - 8.3 The Administrator will lock the screening/registration list away after the service for a period of two weeks.
  - 8.4 The Administrator will shred the lists after two weeks.



## 9. Info desk Sale Receipts

- 9.1 Receipts are collected by an Info Desk volunteer and are placed into an Info Desk folder.
- 9.2 The Team Leader ensures that the Info Desk folder is placed in the safe after the Sunday services.
- 9.3 Receipts are collected by the Finance staff member.
- 9.4 The Finance staff member reconciles receipts, which are shredded thereafter.

## Connect Groups

### 1. New connect Group leader applications:

- 1.1 These are received via website (Disclaimer in place)
- 1.2 These are then sent to the staff member via email.
- 1.3 Information is captured on our Connect Groups Google Sheets document.
- 1.4 Group leaders are informed they will be cared for by a Connect Group leader and contact details are shared with that Connect group leader. A protection of information form is signed by the Connect leader, to ensure the protection of the individuals information.
- 1.5 Connect Group Leaders are added to the Connect Group Leaders WhatsApp Broadcast group.
- 1.6 Any communication to groups of leaders is conveyed via WhatsApp Broadcast groups. The Connect group coordinator is the only one who has access to the connect leaders name, surname and cell number.

### 2. People joining Connect Groups:

- 2.1 All Connect Groups are now listed on the Connexions Church Website.
- 2.2 People joining can register for a group via the website and provide their information willingly.
- 2.3 The Administrator will update the Anatomy groups accordingly.
- 2.4 The Administrator will give the contact numbers of the people who will be joining each group to the leader of each group. (By selecting to "Opt in" people have given their consent for their contact details to be passed on to relevant church leaders)
- 2.5 Each connect group leader will set up a Whatsapp group or broadcast list for their own group. Should a group be set up, then the disclaimer below will be sent to each group member before adding them to the whatsapp group "I hereby give my consent to be added to a whatsapp group for my Connect group for the duration of this term. I acknowledge that my number will be visible to all other members of this group. I will not share any data without gaining the consent of that person. I state my consent below."

## Funerals

1. Personal Information, that is relevant to arranging a funeral, is willingly supplied by the family of the deceased. It will be provided manually or electronically to the Administrator.



2. The family will receive a POPIA compliance form to sign, which gives the administrator permission to process their information.
3. If the family is not a member of Connexions Church, a fee will be charged. They are issued with an invoice from Connexions which may contain their personal information. The invoice procedure is the same as the Finance guidelines.
4. A list of attendees will be requested, for registration and screening to ensure Covid-19 protocol is adhered to. This list will be scanned, saved on the Administrators' password protected computer. Once saved the registration form is shredded.
5. All information is saved on an external drive, which is stored in the safe.

## **Pastoral**

1. The Administrator receives email, website and WhatsApp prayer requests.
2. The Administrator responds directly and then forwards these to the Pastoral staff member.
3. The Pastoral staff member may then determine to share contact information with a member of the Pastoral Team to contact the person and pray with them directly.
4. Information can only be obtained or used with the permission from the person needing prayer or counsel.
5. Permission documents need to be signed by the counselee, providing permission to the Pastoral services person to share relevant information with and only with leadership and Lead Pastors.
6. Every session is documented and stored in a file off site. The POPIA is followed and adhered to, to protect the rights of the pastoral services team and counselee.
7. The counselee is provided with a demographic questionnaire (information provided on this questionnaire is regarded as confidential), POPIA compliance form,
8. Confidential documents from the counselee's are scanned and saved on an external drive which is kept in the safe.
9. Documents are destroyed after 3 months. The documents are kept in a file off site.

## **Courses & Events**

1. Registration for courses and events come in via the website registration system.
2. These are received by the Administrator on a password protected computer.
3. These details are compiled and sent to the course or event coordinator.
4. Communication via email or phone is set up from there.

## **Worship & Production**

1. An individual completes online form or GROW form for data capture.
2. This information is automatically captured into a database.
3. The database is password and permissions protected.

## **Young Adults Connect**

1. Same as Connect Group procedure

## **Reception**



1. If someone calls asking for a staff member's personal information, the Administrator will not give it out and will rather take down the caller's number and convey a message to the relevant staff member.
2. The Administrator will then WhatsApp the staff member the information of the person so that the staff member can call them back.

## Connect Youth

1. Under Covid regulations: People will register via the website link, or in person upon arrival.
2. Under normal circumstances: Parents will write their own and the youth's information down at the registration tables on arrival – a Disclaimer is present on the registration forms.
3. Information provided on registration is then used to add registrations to a spreadsheet, on a password protected computer, an email mailing list and a Youth parents and Teens Broadcast WhatsApp group.
4. Their information will also be added to a registration spreadsheet for the following week.
5. Registration forms are stored in a locked cupboard or scanned and saved electronically on a password protected computer.
6. Details are loaded onto a separate excel database, on a password protected computer, on Mondays.
7. After use, forms are destroyed.

## WordPress

1. Disclaimer to be put in T's & C's for every event that we can use their information (see addendum).
2. Event or service registration:
  - 2.1 People will register for the event or service on WordPress, via our website.
  - 2.2 We will print out the guest list for the event from Wordpress.
  - 2.3 After use, this list is locked away.
  - 2.4 Registration pages are destroyed within a week.

## Anatomy Database

1. Our database is maintained on Anatomy. All staff have access to Anatomy but may not make any changes. Should changes be needed, these may only be made by the designated Anatomy team.
2. Information on our database is taken from a number of sources: Guest forms, Partnership forms, Kids Connect forms and other. This information will be updated every 2<sup>nd</sup> year after an "Up-dating our database" campaign for a month.
3. The Administrator will send out a daily message on the staff WhatsApp group with birthday notifications for people who are on the Anatomy "Active" list. Staff may then connect with these people in their individual capacity.
4. Connect group leaders no longer have access to anatomy. They will only have access to the app to add details of their meetings.
5. The Anatomy protocol includes a clear procedure for the adding of details to our Contacts list and Anatomy database. The procedure is different for people with and without Kids Connect children.



## Kids Connect

1. All people who are 18 years old and over, who are serving at Kids Connect are annually vetted and have police clearance.
2. Check in team members collect password protected laptops from a locked venue.
3. Kids are checked in using our Anatomy database.
4. Following the Sunday services, laptops are switched off and stored in a locked venue.
5. First time guests complete a hard copy Info and Safety form on arrival. This form contains an Opt In/Out option and a POPIA disclaimer This information is locked away after services.
6. The Kids Church pastor contacts parents who have selected to opt in on a Monday and then adds information from the form to Anatomy (as per the Anatomy protocol) The forms are scanned to a password protected computer and the hard copies are shredded.
7. Name stickers are given to all children and parents. These stickers are issued at check in and then taken from parents and children at collection time. Stickers are then destroyed immediately.
8. Barcode cards are issued to parents for check in purposes. These contain parents and children's names and cell phone numbers. These cards are kept in a locked cupboard at Kids Connect prior to being issued to parents for their safekeeping.

## IT

1. Firewall monitored on a daily basis with alert notifications "Switched On" for real time updates.
2. All important documents are stored in a secure Google Cloud Storage solution.

## Communication

- Nearly all communication is done via WhatsApp broadcast lists. By signing the "Opt in" clause on forms people give their permission for the church to give their details to leaders and staff as necessary. On a WhatsApp broadcast, contact numbers are only visible to the administrator of the list and so there is no breach of POPIA.
- There are specific ministries where a WhatsApp group is deemed necessary for communication within the group. These are: Staff, Worship ministry, Elders, Executive staff and Pastoral care. These groups have a disclaimer placed on them which all must agree to. This disclaimer is reposted whenever a new person is added to the group. "I hereby give my consent to be added to the ----- (state name of group) WhatsApp group. I acknowledge that my contact number will be visible to all other members of this group. I will not share any contact numbers without gaining the consent of that person. I state my consent below."

## FINANCIAL SERVICE PROVIDERS

1. First National Bank Privacy Policy

<https://www.fnb.co.za/about-fnb/legal-matters/privacy-policy.html>

2. YOCO Privacy Policy

<https://a.storyblok.com/f/111633/x/34c2d5b842/privacy-policy-and-app-terms-of-use.pdf>



### 3. Snapscan Privacy Policy

<https://www.snapscan.co.za/privacy-statement.html>

## GENERAL SERVICE PROVIDERS

### 1. Wordpress

<https://automattic.com/privacy/>

### 2. Anatomy Privacy Policy

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

### 3. SARS Privacy Policy

<https://www.sars.gov.za/privacy-policy/>

### 4. Investec Privacy Policy

[https://www.investec.com/en\\_za/legal/privacy-policy.html](https://www.investec.com/en_za/legal/privacy-policy.html)

### 5. Ricoh Privacy Policy

<https://www.ricoh.co.za/privacy-policy>

### 6. SAGE Privacy Policy

<https://www.sage.com/en-za/legal/privacy-and-cookies/protection-of-personal-information/>

### 7. AFRIHOST Privacy Policy

[https://www.afrihost.com/site/page/privacy\\_policy](https://www.afrihost.com/site/page/privacy_policy)

### 8. Finsure Privacy Policy

<https://finsure.com.au/privacy-policy>

### 9. Liberty Privacy Policy

<https://www.liberty.co.za/legal>

### 10. CMS Privacy Policy

<https://www.proudlycms.co.za/pdf/cmsalertsprivatepolicy.pdf>

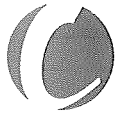
### 11. Dropbox

<https://dropbox.com/privacy>

### 12. Google Drive

<https://policies.google.com/privacy>

### 13. Apple ID Privacy Policy



# CONNEXIONS

011 849 6012

info@connexionschurch.co.za

[www.connexionschurch.co.za](http://www.connexionschurch.co.za)

<https://www.apple.com/legal/privacy/en-ww/>