Churches and Privacy - why should we bother?

First off, the **Legal aspect:**

- In March 2014, the Government introduced the Australian Privacy Principles, which outlines how organisations should be handling people's personal information.
- While only organisations with an annual turnover of $3 million + need to abide by the APPs, these principles are a good outline for how churches can handle information to respect people's privacy.

Now **Biblically,** one part of scripture stands out to me - **1 Peter 2:13-17** it reads**:**

- ***13*** *Submit yourselves for the Lord's sake to every human authority: whether to the emperor, as the supreme authority,* ***14*** *or to governors, who are sent by him to punish those who do wrong and to commend those who do right.* ***15*** *For it is God's will that by doing good you should silence the ignorant talk of foolish people.****16*** *Live as free people, but do not use your freedom as a cover-up for evil; live as God's slaves.* ***17*** *Show proper respect to everyone, love the family of believers, fear God, honor the emperor.*
- We are to submit to every human authority, for it is God's will that by doing good you should silence the ignorant talk of foolish people. Live as free people, but do not use your freedom as a cover-up for evil. Show proper respect to everyone.

The final reason as to why we should bother, is that there are tools available which make it easier to respect people's privacy, why not utilise them?

Church Management Software:

- Elvanto is a great tool in respecting people's privacy because it centralises where your church stores data. Rather than each leader within the church having the details they need on someone, on their laptop, in a spreadsheet. Elvanto is great for storing all of that information in the cloud. It is secure, and you can easily lock down who has access to what details.

APP Summary

I'm now going to take you through a summary of the APPs. Because I believe they are helpful in thinking through how to respect people's privacy within our churches.

As I mentioned before, the Australian Privacy Principles were introduced in March 2014. There are 13 principles in total, which are split into 5 parts. I'll summarise them for you, then provide aspects for you to think about, along with a practical application of the principles in a church context.

Part 1 – Consideration of personal information privacy

APP 1 *- Open and transparent of personal information*

- The object of this principle is to ensure that entities manage personal information in an open and transparent way
  - Basically we should be very open about what we're collecting, and why

APP 2 *- Anonymity and pseudonymity*

- Individuals must have the option of not identifying themselves, or of using pseudonym (fictitious name) when dealing with the church in relation to a particular matter.

<u>Something to think about:</u>

- Is it worth having a privacy policy for your church? I think you should at least have a summary on your website, where someone can go and learn about what information your church collects on them, why that information is collected, where it is stored, and who can they ask about accessing the information stored on them.

Practical Application:

- A disclosure could be placed on the resources used to collect information, and where members can access the privacy policy. For example:
  - To view our privacy policy, go to www.crossroadshobart.org/privacy or contact the office info@crossroadshobart.org
- Also, it would be worth having a contact form on your website where people can anonymously contact you (with the option to provide contact details if they need a response)

Part 2 – Collection of personal information

APP 3 - *collection of solicited personal information (this is where we ask for or try to obtain their information)*

- The following needs to apply, for us to be able to collect sensitive information:
  - The individual must **consent** to the collection of the information
  - The information being collected must **relate** to the activities being undertaken
  - The information must **relate solely to members of the organisation**, or to individuals who have regular contact with the organisation in connection with its activities.
- Also, we must collect personal information only by lawful and fair means.

APP 4 - *dealing with unsolicited personal information (they haven't given their information voluntarily)*

- If we receive information that was not asked for (and not needed), we need to take steps in de-identifying the document or destroying it if it is not necessary for our use.
  - Example: You receive a working with Children card receipt, but only need the card number and expiry date once someone receives their card, the receipt should be de-identified, and or destroyed. Unless it's needed for reimbursement.

APP 5 *- notification of the collection of personal information*

- If personal information comes into our possession that was obtained from a source other than the individual, or the individual may not be aware that we collected their personal information, we need to notify them as soon as practical.

Something to think about:

- Does the information your church collects, relate to the activities being undertaken?
  - If not, you may need to think about auditing your ministries, to make sure they're only collecting the information they need to undertake their ministry.

Practical Application:

- This is the only catchy application I could think of, 'Collect people's emails, not their social networking details'. When collecting people's details, it probably wouldn't be appropriate to ask if they have a Facebook, Instagram, or Twitter account. While this might be helpful to know in some instances, most churches wouldn't need to know each member's social networking information.

Part 3 – Dealing with personal information

APP 6 – *Use or disclosure of personal information*

- If we hold personal information that was collected for a particular purpose, we must not use or disclose the information for another purpose unless:

    - The individual has consented to the use or disclosure of the information.
    - Or, the individual would reasonably expect us to use the information for the other purpose.
        - for example – we collect an email address to add to an email list, it would be reasonable for us to then update the email address in the database, which would then update the directory.
- This probably wouldn't happen, but if we do disclose personal information to an enforcement body for an enforcement related activity, we must make a written note of the use or disclosure.

APP 7 *– Direct Marketing*

- We are not allowed to disclose personal information for the purpose of direct marketing, or government related identifiers.
    - Unless the information is collected by us, and the individual consents to the use of it in direct marketing.
    - So we should de-identify any information passed out to other parties (for statistics, etc).

APP 8 *– cross-border disclosure of personal information*

- If we are passing on personal information to overseas parties, we need to ensure that that party is not breaching the APPs

APP 9 *– adoption, use or disclosure of government related identifiers*

- We must not use government related identifiers (Centrelink numbers, etc), unless it is required by law.
    - The main example I can see here, is that churches need to take note of Working With Vulnerable Children number, but probably do not need people's Centrelink numbers.

Something to think about:

- Does your church use third party applications like Google docs, or Mail Chimp, in your day-to-day operations?
    - It may be worth letting people know in your privacy policy/disclosure about the use of these applications, and where they can look for information about the security of information within these applications.

Practical Application:

- Only use personal information that we collect for that specific reason.
    - If we need to collect the same information more than once, that is ok, as it provides us with the opportunity for the person to consent for the second reason.
- Ensure that all marketing material containing personal information (phone numbers/emails), is used with the individual's consent.
    - If you don't have their consent by the time of publication, then remove their details until a time in which you have received their consent.
- DON'T give personal information to overseas parties.
    - If it is necessary, seek the individual's consent.
        - For example, to complete a working with children application, one of the pastors in the Network needed to get a background check from America, meaning that I had to fax through their personal details to the FBI. I obviously had his consent as he had filled in the form and asked me to send it.
- Only acquire government related identifiers that are required by law.
    - Such as WWC number & expiry

  - Drivers licence (for insurance purposes)
  - Any other details required for medical permission forms.

Part 4 – Integrity of personal information

APP 10 – *quality of personal information*

- We need to take reasonable steps to ensure that the information that is collected/disclosed, is accurate, up to date, and complete.

APP 11 – *security of personal information*

- We need to take reasonable steps to ensure that the information collected is protected from misuse, interference and loss; and from unauthorised access, modification or disclosure.
- If we hold personal information that is no longer needed, we need to ensure it is destroyed or de-identified.

Something to think about:

- How are you ensuring the information you have in Elvanto is up to date?
  - This is not only helpful for the directory (if your church has/uses one), it can also save a lot of admin effort, trying to source a person's contact details
- Who within your congregation has access to people's personal information?

Practical Application:

- Send out regular (once/twice yearly) enquiries for up to date information from members.
- Ensure all computers that have access to personal information are password protected (even personal computers).
- For information stored in Elvanto that you may no longer need, have a procedure of archiving the personal information for a period, then deleting it after a set period.

Part 5 – Access to, and correction of, personal information

APP 12 – *access to personal information*

- We need to be able to give a person access to the information that we have stored about them.
- We must deal with a response for personal information within a reasonable time, and if it is reasonable and practical to do so.
  - If we refuse the person access to personal information, we must give written notice that sets out:
    - The reasons for the refusal
    - How they can make a complaint about the refusal
    - Any other matter prescribed by the regulations

APP 13 – *correction of personal information*

- If we believe the information held is inaccurate, or the individual requests us to correct the information stored, we must take reasonable steps to update the information.
- If we correct information that has been disclosed to another party, we need to notify them of the correction.
- If we refuse to correct information as requested by an individual, we need to give them written notice that sets out.
  - The reasons for the refusal
  - How they can make a complaint about the refusal

    - Any other matter prescribed by the regulations
- We must not charge the individual for the making of the request, or for correcting the personal information.

Something to think about:

- Who is responsible in your church for receiving requests about personal information, or correcting information?

Practical Application:

- Provide an avenue, either on your website, or in your privacy policy/disclosure, for people to contact about any of the above.

With all of this in mind, I'm now going to walk you through an information pathway, where information is collected, is handled, and removed/archived within Elvanto.

Information pathway

- One feature of Elvanto is webforms. It's quite smart in that you can create a form, then when someone fills in the form online, it will either create a profile for that person that filled it in. Or, if they are already in your church's system, it will notify you of different details that person may have put in, for example a different mobile number from their current one, and ask you whether you would like to update their current profile.
- One limitation to the webform, is that it can only collect one person's details at a time. So a family of four people, would have to fill in the same form four times. To address this, the IT Team have developed our own webform, that can collect a family of up to 10 people's details in one form. While this method requires a bit more work for the administrators within the church, we believe that it will be more successful in getting people to fill out this single form, over an Elvanto form however many times for their family.

For the walkthrough, I'm going to take you through Crossroads webform and Elvanto setup.

Church Webform

- http://crossroadshobart.org/memberinfo
- Walk people through the webform (what information is being collected).
- Once you hit submit, the first thing you'll need to think about in terms of privacy, is who will be collating all of the information coming in, and transferring it into Elvanto. You'll need to discuss with that person the importance of confidentiality.
- I won't take you through the import process, that's something we can take you through on an individual church basis.

Profile

- The big privacy concern with a profile in Elvanto, is who has access to what information. Thankfully in Elvanto, you can lock down the access permissions, so the person on the setup packup roster can't log in and see the pastoral notes written about someone.

Information pathway within Elvanto

- So, say Chris and his family have just joined the church. They go from being visitors, to adherents, to church members, then decide to move away. What should you do with the information?
    - They want to stay updated:
        - Mark them as contacts and place in the Past Members category
    - They want to cease electronic communication

        - Mark them as contacts and place in the inactive category, for maybe 12 months. Then at the beginning of each year, delete those in the Inactive category (or set a reminder of once moved to Inactive category, email me in 12 months to delete them).
- You need to be thinking about every step of Chris and family going from visitor through to church member. Who has access to their information, etc.

Privacy tips for:

- Leadership
    - Unless the leader is overseeing a ministry, they should probably only have access to the details of those they're pastorally caring for.
    - The respecting privacy culture starts with the leadership. If a member sees or hears of a leader passing on information, they will think it's ok.
- Ministry Leaders
    - They should be able to only see who they directly oversee. When a person signs up to serve, the ministry leader should mainly be accessing personal information for contacting them, or seeing their availability/unavailability, rather than other unnecessary information.
    - Let people know when they sign up for rosters, that their contact details will be made available for other people on the same roster to contact them
- Members
    - Not all members will want their details shared. We should respect that, and check what some of the reasons for not sharing their information may be. There might be concerns that we can easily address, so that they have confidence in their data (such as contact information) being shared with others in the church.
    - Assure them about their details when they give them to the church, they will be handled securely and respectfully.
- Visitors
    - Visitors will probably be the most suspicious about you collecting their details (unless they have signed up for an event). You need to make sure you can explain to them exactly why you're collecting the information that you are. E.g. You collect their email so you can send them a follow up email, or add them to your church's mailing list.
    - Only people overseeing pathways within your church should have access to these details, until they willingly give you more of their details.

Other practical tips for respecting people's privacy:

- Think through who actually needs access to people's data
    - Sometimes, the less people who have access the easier.
        - Rather than give every person access to their profile, it might be best to leave leaders within the church to change details.
- Encourage a culture of asking before passing on information. As it's best if we can avoid offending someone because their mobile number or email address got passed on without them knowing/approving.