Appendix 3 - Audit Questionnaire

To be used for Record keeping

This form is designed to help Fountain of Peace Ministries (FOP) to audit their personal data processing. It is important to complete this form as comprehensively as possible.

"Personal Data" is any information about a living person which can identify them. This is not just someone's name and address but any ID information. For example a phone number or email address is personal data. Any other contact information or a person's employment history, medical conditions, criminal record or credit history are all personal data.

'Processing' personal data means storing or deleting any personal data on a computer, database or some manual files (e.g. HR personnel files). The word 'processing' also covers selecting a name for a mailing list, or reading it off a screen during a sales call. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing.

Appendix 3

Part	YOUR INFORMATION	
1.	1. Person completing questionnaire	
	a) Name.	
	b) Role.	
	c) Telephone extension number. d) Email.	
2.	Data controller (e.g. Fountain Of Peace Ministries)	
3.	Date you completed this survey	
Part	COMMUNICATIONS DATA	
4.	This section relates to communications with church members and other churches and organisations including contacts (e.g. via outreach activities, weddings, baptisms, funerals). Communications include mailing lists for Water of Life/Newsletters or requests for donations: **a)** What type of information do we keep? E.g. Name, contact details Gift Aid information and congregational giving details such as bank details. **b)** Where do we get the data from? E.g. individuals themselves, family members, clergy, other church sources, publicly available sources e.g. electoral register. **c)** Why do we collect or process the data - what do we do with it? For purposes relating to: e.g. church membership, and for contact regarding involvement in parish activities; advertising, outreach programmes *[Please list all reasons],* **d)** Who do we disclose communications data to? E.g. Senior Pastor, church members and contacts carrying out the work of the church, colleges, other church organizations. **e)** Do we ever send communications data overseas and if so where to and to which company? This might include overseas companies providing database or email services. E.g. linked branches, mission agencies, cloud storage	
Part	SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS WE DO WITH	

5.	About individuals or representatives of organizations which supply us with services such as for church repairs, or with whom we are in contact **a)** Who do we keep personal data about? E.g. Trades people, surveyors, architects, builders, suppliers, advisers, payroll processors, donors to appeals [Please list any others]. **b)** What type of information do we keep? E.g. Name, contact details, qualifications, financial details, details of certificates and diplomas, gift aids, education and skills [Please list any others]. **c)** Where do we get the data from? E.g. the individuals, companies, suppliers [Please list any others]. **d)** Why do we collect or process the data? E.g. church repairs and upkeep; maintain services e.g. electrical, gas,	
Part D: GENERAL QUESTIONS ABOUT PERSONAL DATA		
6.	How do we store the personal data collected? Do we take any steps to prevent unauthorized use of or access to personal data or against accidental loss, destruction or damage? If so, what? How do we manage access to data - what is the process involved in getting access?	
7.	Do any procedures exist for rectifying, deleting, suppressing or blocking, personal information? If so, please provide details.	
8.	Who has access to / is provided with the personal data (internally and externally)? Is there an authorization procedure for accessing personal data? If so, please provide details.	
9.	Can we provide a copy of all existing data protection or privacy notices and consents used?	
10.	So far as we are aware, has any personal data, which was gathered for one purpose (e.g. electoral roll membership) been used for another purpose (e.g. circulating details of church services& activities? If so, please provide details.	
11.	Are we aware of any policies, processes or procedures to check the accuracy of personal data?	
12.	In the event of a data security breach occurring, does the FOP have in place processes or procedures to be followed? What are these?	
13.	If someone asks for a copy of information that the church holds about them, i.e. they make a 'subject access request', is there a procedure for handling such a request? Who do we send the request to?	

14.	Can we locate a copy of the 'consent[1] language currently used for communications?	
15.	Are cookies used on our church website? If so, can we provide a copy of the form of consent used? Do we allow individuals to refuse to give consent? Do we provide information about the cookies used and why they are used?	
16.	Are any communications files, which may be used, checked against marketing suppression lists where relevant, such as the Mailing Preference, Fax and Telephone Preference Services?	
17.	Can we provide a copy of all website privacy notices and privacy policies?	
18.	What data protection training do people in the FOP and other key data users (e.g. church administrator, Sunday school co-coordinator, youth leader, stewardship officer, hall bookings secretary) receive? What does the training involve?	
19.	Does anyone in the FOP have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date? If so, how regularly are these activities carried out?	
20.	What do we do about archiving, retention or deletion of personal data?	
Part E: PERSONAL DATA		

Appendix 3

21.	This is intended as a full coverage of the FOP personal data and processing activities, which is in addition to (rather than repeating) information provided in Parts B and C. **a)** Who do we keep personal data about? E.g. Church role and office holders (such as churchwardens, FOP Secretaries, Apostolic council members, Trustee members, church Safeguarding officer, Sunday School coordinator, youth leaders/workers), church members, Day Centre volunteers (FDC), children, youth, staff, employees, hall hirers, and contractors. [Please list anyone else] **b)** What type of information do we keep? E.g. Name, contact details, date of birth, child registration information, Safeguarding information, information on employees. [Please list anything else] **c)** Where do we get the data from? E.g. The individuals themselves, other churches, district authorities, National Church, Deanery officers companies and recruitment agencies. [Please list anyone else] **d)** Why do we collect or process the data? E.g. To further the mission and ministry of the church including by carrying out activities, advertising services and events, outreach program, employee administration and payroll; operational reasons. [Please list anything else] **e)** Do we collect any sensitive information (other than religious beliefs): Relating to racial or ethnic origin, political opinions, trade union membership, physical or mental health or criminal records? If so for what reason: e.g. criminal records for Safeguarding compliance; physical or mental health information relating to employees; racial and ethnic origin relating to equal opportunities monitoring. [Please list anything else] **f)** Who do we disclose the data to? E.g. Senior Pastor, church members and contacts carrying out the	

22.	Please identify any monitoring of the following systems that takes place. 'Monitoring' includes all monitoring of systems including without limitation intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are: (a) Computer networks and connections (b) CCTV and access control systems (c) Communications systems (d) Remote access systems	

Appendix 4 -GDPR Consent Form

CONSENT FORM

"Your privacy is important to us and we would like to communicate with you about the church and its activities. To do so we need your consent. Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below."
How we use your personal data is on our privacy notice which you can find here: [http://www.fountainofpeace.org/].

If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent

Name…….
Address…….
Signature……...
Date……

Please confirm your consent to one or more of the following[1]:

Newsletters and other communications
We may contact you to keep you informed about what is going on in the local or neighboring branches, other churches and the work of the Head quarter including news, events, conference and convention, cell groups, and other activities. These communications may also sometimes appear on our website or in printed or electronic form (including social media).

Activities and groups
We may contact you about groups and activities you may be interested in participating in. We sometimes work with similar groups in other churches within or outside our church. Occasionally names and photos may appear in newsletters, Water of Life, tracks or on websites, CD/ DVD, or social media. Keeping in touch

- □ **Yes please, I would like to receive communications by email**
- □ **Yes please, I would like to receive communications by telephone**
- □ **Yes please, I would like to receive communications by mobile phone including text messages**
- □ **Yes please. I would like to receive communications by social media**
- □ **Yes please, I would like to receive communications by post**

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events; except in certain limited situations, such as where required to do so by law or protect members of the public from serious harm. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Church Office or at [http://www.fountainofpeace.org/ You can withdraw or change your consent at any time by contacting the Church Office.

Appendix 5 - Privacy Notices

GENERAL PRIVACY NOTICE

(Note: This Privacy Notice is for non-role holders. See explanatory note on Privacy Notices on p.8)

Your personal data - what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by ***[the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998],***

Who are we?

This Privacy Notice is provided to you by the FOUNTAIN OF PEACE MINISTRIES (FOP) of which is the data controller for your data.

- **the incumbent of the pastor ; [Snr Pastor or Associate Pastor);**
- **the ministers of the Fountain of Peace; and**
- **Apostolic council member's, which are responsible for the financial and administrative arrangements for the church.**

As the Church is made up of all of these persons and groups working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The groups referred to above are joint data controllers. This means we are all responsible to you for how we process your data. Each of the data controllers have their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the FOP on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word "we" to refer to each data controller, as appropriate.

What data do the data controllers listed above process? They will process some or all of the following where necessary to perform their tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependents;
- Where you make donations or pay for activities such as use of a church hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process is likely to constitute sensitive personal data because, as a church, the fact that we process your data at all may be suggestive of your religious beliefs. Where you provide this information, we may also process other categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received,

Political beliefs, labor union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

How do we process your personal data?

The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorized access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

We use your personal data for some or all of the following purposes:

- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our pastoral roll in accordance with the Church Representation Rules);
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To minister to you and provide you with pastoral and spiritual care (such as visiting you when you are gravely ill or bereaved) and to organize and perform ecclesiastical services for you, such as baptisms, confirmations, weddings and funerals;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the church, deanery, archdeaconry and diocesan membership records;
- To fundraise and promote the interests of the Church and charity;
- To maintain our own accounts and records;
- To process a donation that you have made (including Gift Aid information);
- To seek your views or comments;
- To notify you of changes to our services, events and role holders;

- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

- Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another groups in the Church - FOP). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.
- Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banns.
- We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.
- Religious organizations are also permitted to process information about your religious beliefs to administer membership or contact details.
- Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties where it is necessary for the performance of our tasks or where you first give us your prior consent. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The appropriate bodies of FOP including the other data controllers;

- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
- Other pastors or ministers nominated or licensed by the snr pastor of the Fountain of Peace ministries to support the mission of the Church. For example, officiating ministers, who may provide confidential mentoring and pastoral support often support our snr pastors. Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with Snr Pastor's Permissions may participate in our mission in support of our regular services.
- Other persons or organizations operating within the Fountain of Peace ministries including, where relevant, the Fountain College and Fountain Day Centre;
- On occasion, other churches with which we are carrying out joint events or activities.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavor to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:
When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. **The right to access information we hold on you**

- At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.

- There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee .

2. **The right to correct and update the information we hold on you**
   - **If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.**

3. **The right to have your information erased**
   - If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
   - When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

4. **The right to object to processing of your data**
   - You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.
   -

5. **The right to data portability**
   - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.**
   - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. **The right to object to the processing of personal data where applicable.**

8. **The right to lodge a complaint with the Information Commissioner's Office.**

Appendix 6

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter or Water of Life) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:
The Data Controller, [Mark Amadi]
Email: academy@fountainofpeace.org

Appendix 6

PRIVACY NOTICE

ROLE HOLDERS

(e.g. Administrative Dept, FOP Secretaries, FOP Treasurers, Pastoral Care Office,

See explanatory note on Privacy Notices on p.8)

Your personal data - what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by ***[the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998],***

Who are we?

This Privacy Notice is provided to you by the Fountain of Peace Ministries (FOP), who is the data controller for your data. FOP is made up of a number of different groups and office-holders who work together to deliver the Church's mission in the community. The FOP works together with:

- **the incumbent of the Church [Snr Pastor/Pastor];**
- **Apostolic Council;**

As the Church is made up of all of these persons and organizations working together, we may need to share personal data we hold with them so that they can carry out their responsibilities to the Church and our community. The group/team referred to above are joint data controllers. This means we are all responsible to you for how we process your data.

Each of the data controllers has their own tasks within the Church and a description of what data is processed and for what purpose is set out in this Privacy Notice. This Privacy Notice is sent to you by the FOP on our own behalf and on behalf of each of these data controllers. In the rest of this Privacy Notice, we use the word "we" to refer to each data controller, as appropriate.

Appendix 6

How do we process your personal data?

The data controllers will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorized access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

We use your personal data for some or all of the following purposes (for example some of the role- holders are volunteers and no financial information will be processed for these role holders): -

- To enable those who undertake pastoral care duties as appropriate (e.g. visiting the bereaved);
- To enable us to meet all legal and statutory obligations (which include maintaining and publishing our electoral roll in accordance with the Church Representation Rules);
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments;
- To deliver the Church's mission to our community, and to carry out any other voluntary or charitable activities for the benefit of the public as provided for in the constitution and statutory framework of each data controller;
- To administer the church membership records;
- To fundraise and promote the interests of the church and charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records;
- To seek your views or comments;
- To notify you of changes to our services, events and role holders
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other fundraising activities;
- To process a grant or application for a role;
- To enable us to provide a voluntary service for the benefit of the public in a

particular geographical area as specified in our constitution;

- To share your contact details with the various groups of the church so they can keep you informed about news within and outside the church and events, activities and services that will be occurring in church in which you may be interested.
- We will process data about role holders for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations, for example to pay role-holders, monitor their performance and to confer benefits in connection with your engagement as a Role Holder. "Role Holders" includes volunteers, employees, contractors, agents, staff, retirees, temporary employees, beneficiaries, workers, treasurers and other role holders.
- We may process sensitive personal data relating to Role Holders including, as appropriate:
    - *information about an Role Holder's physical or mental health or condition in order to monitor sick leave and take decisions as to the Role Holder's fitness for work;*
    - *the Role Holder's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;*
    - *in order to comply with legal requirements and obligations to third parties.*
- Our processing also includes the use of CCTV systems for the prevention and prosecution of crime.

What data do the data controllers listed above process?

- Names, titles, and aliases, photographs.
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our mission, or where you provide them to us, we may process demographic information such as gender, age, date of birth, marital status, nationality, education/work histories, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving license numbers,

vehicle registration numbers, taxpayer identification numbers, employee identification numbers, tax reference codes, and national insurance numbers.

- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as salary, bonus, record of earnings, tax code, tax and benefits contributions, expenses claimed, creditworthiness, car allowance (if applicable), amounts insured, and amounts claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Other employee data (not covered above) relating to Role Holders including emergency contact information; gender, birth date, referral source (e.g. agency, employee referral); level, performance management information, languages and proficiency; licenses/certificates, citizenship, immigration status; employment status, retirement date; billing rates, office location, practice and specialty; publication and awards for articles, books etc.; prior job history, employment references and personal biographies.
- The data we process is likely to constitute sensitive personal data because, as a church, the fact that we process your data at all may be suggestive of your religious beliefs. Where you provide this information, we may also process other categories of sensitive personal data: racial or ethnic origin, sex life, mental and physical health, details of injuries, medication/treatment received, political beliefs, labor union affiliation, genetic data, biometric data, data concerning sexual orientation and criminal records, fines and other similar judicial records.

What is the legal basis for processing your personal data?

Most of our data is processed because it is necessary for our legitimate interests, or the legitimate interests of a third party (such as another organization in the Church). An example of this would be our safeguarding work to protect children and adults at risk. We will always take into account your interests, rights and freedoms.

Some of our processing is necessary for compliance with a legal obligation. For example, we are required by the Church Representation Rules to administer and publish

the electoral roll, and under Canon Law to announce forthcoming weddings by means of the publication of banners.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the hire of church facilities.

We will also process your data in order to assist you in fulfilling your role in the church including pastoral and administrative support or if processing is necessary for compliance with a legal obligation.

Religious organizations are also permitted to process information about your religious beliefs to administer membership or contact details.

Where your information is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

Sharing your personal data

Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with

- The appropriate bodies within the church management stakeholders;
- Our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software;
- Other pastoral team or duty ministers to support the mission of the Church. For example, our ministers provide confidential mentoring and pastoral support. Assistant or temporary ministers, including curates, deacons, licensed lay ministers, commissioned lay ministers or persons with senior pastor may participate in our mission in support of our regular ministrations;

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC

audits. In general, we will endeavor to keep data only for as long as we need it. This means that we may delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. **The right to access information we hold on you**

- At any point you can contact us to request the information we hold on you as well as why we have that information, who has access to the information and where we obtained the information from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.

2. **The right to correct and update the information we hold on you**

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. **The right to have your information erased**

- If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.
- When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

4. **The right to object to processing of your data**

- You have the right to request that we stop processing your data. Upon receiving the request we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you

exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

5. **The right to data portability**

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought.**

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. **The right to object to the processing of personal data where applicable.**

8. **The right to lodge a complaint with the Information Commissioners Office.**

Transfer of Data Abroad

Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on **this web page;** http://www.fountainofpeace.org/privacy-policy/. This Notice was last updated in May 2018.

Appendix 6

Contact Details

Please contact us if you have any questions about this Privacy Notice or the information we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, [Fountain of Peace Ministries]

Email: academy@fountainofpeace.org

Appendix 6 - DPIA Assessment Checklist

The GDPR requires that organizations carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For examples, might include, introducing a new safeguarding protocol which involves sharing data with multiple agencies or using CCTV to monitor public areas.

If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system.

1. Profiling is in use. Example: you monitor website clicks or behavior and record people's interests. ☐
2. Automated-decision-making. Example: when processing leads to the potential exclusion of individuals. ☐
3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐
4. Sensitive data. Examples: information about individuals' political opinions, as well as personal data relating to criminal convictions or offences. ☐
5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐
6. Linked databases - in other words, data aggregation. Example: two datasets merged together, that could "exceed the reasonable expectations of the user". E.g. you merge your mailing list with another church, club or association. ☐
7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. employee-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐
8. "New technologies are in use". E.g. use of social media, etc. ☐
9. Data transfers outside of the EU. ☐
10. "Unavoidable and unexpected processing". For example, processing ☐

Performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking.

A more detailed DPIA Assessment Checklist can be found at

http://www.fountainofpeace.org/privacy-policy/.

Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, organizations need to be able to evaluate when a DPIA is required. This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

Do you need to carry out a DPIA? Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, organizations need to be able to evaluate when a DPIA is required.
This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

Do you need to carry out a DPIA?

- What is the objective/intended outcome of the project?
- Is it a significant piece of work affecting how services/operations are currently provided?
- Who is the audience or who will be affected by the project?
- Will the project involve the collection of new information about people? (e.g. new identifiers or behavioral information relating to individuals?)
- Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?
- Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?
- Is data being processed on a large scale?
- Will the project compel individuals to provide information about themselves?

- Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?
- Will personal information be transferred outside the EEA?
- Is information about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?
- Will information about children under 16 or other vulnerable persons be collected or otherwise processed?
- Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)
- Is monitoring or tracking or profiling of individuals taking place?
- Is data being used for automated decision making with legal or similar significant effect?
- Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behavior)
- Is sensitive data being collected including:
  - Race
  - Ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership
  - Genetic data
  - Biometric data (including facial recognition)
  - Finger or palm print data
  - Health data
- Data about sex life or sexual orientation?
- Will the processing itself prevent data subjects from exercising a right or using a service or contract?
- Is the information about individuals of a kind likely to raise privacy concerns or is it information people would consider to be particularly private or confidential?
- Will the project require contact to be made with individuals in ways they may find intrusive?

- Other issues to consider when carrying out a DPIA
- In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:
- The lawful grounds for processing and the capture of consent where appropriate
- The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing
- Who the data will be disclosed to
- Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)
- The internal process for risk assessment
- Who needs to be consulted (DPO, data subjects, regulator)
- Data minimization (including whether data can be anonymised)
- How accuracy of data will be maintained
- How long the data will be retained and what the processes are for deletion of data
- Data storage measures
- Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk
- Opportunities for data subject to exercise their rights
- What staff training is being undertaken to help minimise risk
- The technical and organizational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behavior or incidents)
- What is the objective/intended outcome of the project?
- Is it a significant piece of work affecting how services/operations are currently provided?
- Who is the audience or who will be affected by the project?
- Will the project involve the collection of new information about people? (e.g. new identifiers or behavioral information relating to individuals?)
- Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?
- Will the project involve combining datasets originating from different

processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?

- Is data being processed on a large scale?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?
- Will personal information be transferred outside the EEA?
- Is information about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?
- Will information about children under 16 or other vulnerable persons be collected or otherwise processed?
- Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)
- Is monitoring or tracking or profiling of individuals taking place?
- Is data being used for automated decision making with legal or similar significant effect?
- Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behavior)
- Is sensitive data being collected including?
    - Race
    - Ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership
    - Genetic data
    - Biometric data (including facial recognition)
    - Finger or palm print data
    - Health data
    - Data about sex life or sexual orientation?
- Will the processing itself prevent data subjects from exercising a right or using a service or contract?
- Is the information about individuals of a kind likely to raise privacy concerns or

is it information people would consider to be particularly private or confidential?

- Will the project require contact to be made with individuals in ways they may find intrusive?
- Other issues to consider when carrying out a DPIA
- In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:
- The lawful grounds for processing and the capture of consent where appropriate
- The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing
- Who the data will be disclosed to
- Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)
- The internal process for risk assessment
- Who needs to be consulted (DPO, data subjects, regulator)
- Data minimisation (including whether data can be anonymised)
- How accuracy of data will be maintained
- How long the data will be retained and what the processes are for deletion of data
- Data storage measures
- Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk
- Opportunities for data subject to exercise their rights
- What staff training is being undertaken to help minimise risk
- The technical and organizational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behavior or incidents)

Appendix 6