All Nations Church

BARKINGSIDE & CLAYHALL

ALL NATIONS CHURCH BARKINGSIDE & CLAYHALL (ANCBC)

Charitable Incorporated Organisation (CIO) registered in England and Wales with charity number 1196151

DATA PROTECTION, INFORMATION SECURITY &

DATA RETENTION POLICY

(the "Policy")

IMPORTANT NOTE

The General Data Protection Regulation (EU) 2016/679 ("GDPR") came into effect on the 25th May 2018. It is important for you to read and understand this Policy as it will give you important information about:

- the data protection principles with which All Nations Church Barkingside & Clayhall (ANCBC) must comply; and
- your obligations as a ANCBC employee, worker or volunteer should you process personal data for ANCBC or for any ANCBC Church and the consequences of failure to comply with this Policy.

Policy Chronology
09/2020 : Policy sent to all staff and relevant volunteers prior to training workshop
Next Review Date: 10/2022

Contents

1. Introduction

1.1. This is the Data Protection, Information Security & Data Retention Policy (the "**Policy**") for All Nations Church Barkingside & Clayhall ("ANCBC") and applies to the ministries resourced through ANCBC.

1.2. This Policy sets out the overarching data protection and information security arrangements for ANCBC and the Churches and the responsibilities of all ANCBC Workers. In this Policy, **"ANCBC Workers"** includes all employees, workers and volunteers serving ANCBC or any of the Churches.

1.3. The Policy sets out standards ANCBC Workers are expected to comply with, but is not contractually binding upon ANCBC nor any Church as part of an individual contract/document governing working terms of ANCBCWorkers. ANCBC may amend it at any time and the Policy will be kept up to date and will continue to be reviewed to ensure it is achieving its aims. To ensure this, the Policy and the way in which it is operated and communicated will be reviewed every two to three years and appropriate changes made.

2. Policy purpose

2.1. The purpose of this Policy is to ensure that all ANCBC Workers:

2.1.1. understand and comply with ANCBC's rules governing the collection and deletion of personal information (also referred to in this Policy as "**data**") to which they may have access in the course of their work;

2.1.2. protect against potential breaches of confidentiality; and

2.1.3. are aware and understand ANCBC's requirements of information security.

3. General Statement of Policy

3.1. ANCBC and the Churches are committed to:

3.1.1. complying with their data protection obligations;

3.1.2. protecting personal information and other confidential information from loss, theft, misuse or inappropriate access or disclosure; and

3.1.3. not retaining personal information for any longer than necessary.

3.2. For the purposes of this Policy, without limitation, "confidential information" includes information (whether received, accessed or viewed by the recipient in writing, visually, electronically or orally):

3.2.1. gained from any source that describes or pertains to an individual's personal, medical, social or financial information;

3.2.2. regarding ANCBC (or one of their ANCBC Workers or members/regulars) that, if lost, stolen or inappropriately released without proper authorisation, could do harm to ANCBC (or to their employees, workers, volunteers or members) and includes (but is not limited to) lists of members, donors, donations and grants, confidential memos concerning counselling sessions, staff information and information about pastoral matters and concerns;

3.2.3. that is marked or otherwise communicated as being confidential (or similar wording) or ought reasonably to be understood to be confidential.

4. Consequences of non-compliance with this Policy

4.1. Failure to comply with this Policy:

4.1.1. puts at risk the individuals whose personal information is being processed;

4.1.2. carries the risk of civil and criminal sanctions for the individuals who process personal information and also ANCBC itself; and

4.1.3. may harm gospel work and damage the reputation of our Lord Jesus and his churches.

4.2. Due to the importance of this Policy, an employee's failure to comply with any requirement of it may lead to disciplinary action and dismissal for gross misconduct. A non-employee who breaches this Policy may have their work/ ministry terminated with immediate effect.

5. Data Protection

5.1. Data Protection Principles

5.1.1. ANCBC and the Churches will comply with the following data protection principles when processing personal data:

(a) they will only process personal data lawfully, fairly and in a transparent manner;

(b) they will collect personal data for specified, explicit and legitimate purposes only, and not process it in a way that is incompatible with those legitimate purposes;

(c) they will only process personal data that is adequate, relevant and necessary for relevant purposes;

(d) they will keep accurate and up to date personal data and will take reasonable steps to ensure that inaccurate personal data is deleted or corrected without delay;

(e) they will keep personal data for no longer than is necessary for the purposes for which the data is processed; and

(f) they will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected from unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5.2. Basis for processing personal data

5.2.1. ANCBC will, in relation to any processing activity of ANCBC or a Church, regularly (e.g. every two to three years) review the purposes of the processing activities and select the most appropriate lawful basis (or bases) for that processing. In most cases the lawful basis will be that the processing is necessary for the purposes of the legitimate interests of ANCBC, a Church or a third party (except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject - see Section 5.2.8 below).

5.2.2. The other lawful bases potentially likely to apply are as follows:

(i) that the data subject has consented to the processing; or

(ii) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps, at the request of the data subject, prior to entering into a contract; or

(iii) that the processing is necessary for compliance with a legal obligation to which ANCBC or a Church is subject; or

(iv) that the processing is necessary for the protection of the vital interests of the data subject or another natural person.

5.2.3. ANCBC will, except where the processing is based on consent, satisfy itself that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

5.2.4. ANCBC will document its decision (see examples in ***Appendix II***) as to which lawful basis applies, to help demonstrate its compliance with the data protection principles.

5.2.5. ANCBC will include information about both the purposes of the processing and the lawful basis for it in its Privacy Policy (which can be found on each Church website).

5.2.6. Where sensitive personal data is processed, ANCBC will also identify a lawful special condition for processing that data (see paragraph 5.3.3(b) below), and document it.

5.2.7. Where criminal offence data is processed, ANCBC will also identify a lawful condition for processing that data, and document it.

5.2.8. When determining whether ANCBC or a Church's legitimate interests are the most appropriate basis for lawful processing, ANCBC will:

(a) conduct a legitimate interests assessment ("***LIA***") and record the outcomes of these assessments (see examples in ***Appendix II)***;

(b) keep the LIA under review, and repeat it if circumstances change; and

(c) include information about ANCBC's legitimate interests in its relevant privacy notice(s).

5.3. <u>Sensitive personal data</u>

5.3.1. GDPR refers to 'special categories of personal data' (Article 9, GDPR) which includes data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included within the special categories of personal data under GDPR but similar extra safeguards apply to its processing (Article 10, GDPR). For the purposes of this Policy data which falls within a special category of personal data and personal data relating to criminal convictions and offences shall be referred to as "**sensitive personal data**".

5.3.2. The data that may be processed by ANCBC or a Church may constitute sensitive personal data because, as churches/ministries, the fact that they process data may be suggestive of religious beliefs (e.g. a photo of an individual being baptised). ANCBC or a Church may also process other categories of sensitive personal data e.g. data concerning health in relation to pastoral care/Sunday School classes/children's clubs/events. They may also process data in relation to criminal convictions and offences in relation to DBS checks/safeguarding obligations.

5.3.3. ANCBC and the Churches will only process sensitive personal data if:

(a) It has a lawful basis for doing so as set out in Section 5.2 above, e.g. it is necessary for the performance of the employment contract, to comply with ANCBC's legal obligations or for the purposes of ANCBC's legitimate interests; and

(b) one of the special conditions for processing sensitive personal data applies, e.g.:

(i) being a not for profit organisation with a religious aim, the processing is carried out in the course of ANCBC/a Church's legitimate activities with appropriate safeguards and the processing relates solely to members (or former members) or others with whom they are in regular contact in connection with its charitable purposes and such data is not disclosed outside of ANCBC and the Churches (Article 9(2)(d)); or

(ii) the data subject has given explicit consent; or

(iii) the processing is necessary for the purposes of exercising the employment law rights or obligations of ANCBC or the data subject; or

(iv) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent; or

(v) processing relates to personal data which is manifestly made public by the data subject; or

(vi) the processing is necessary for the establishment, exercise or defence of legal claims; or

(vii) the processing is necessary for reasons of substantial public interest.

5.3.4. Before processing any sensitive personal data (other than sensitive personal data which is referred to in the examples in ***Appendix II***), ANCBC Workers should first notify their Church Data Protection Lead and/or, if appropriate, the ANCBC Data Protection Lead of the proposed processing, in order that they may assess whether the processing complies with the criteria noted above.

5.3.5. Sensitive personal data will not be processed until the assessment referred to in Section 5.3.3 has taken place.

5.3.6. ANCBC's Privacy Policy sets out the types of sensitive personal data that ANCBC processes, what it is used for and the lawful basis for the processing.

5.4. Data breaches

5.4.1. A data breach may take many different forms, for example:

(a) loss or theft of data or equipment on which personal data is stored;

(b) unauthorised access to or use of personal data either by a member of staff or third party;

(c) loss of data resulting from an equipment or systems (including hardware and software) failure;

(d) human error, such as accidental deletion or alteration of data;

(e) unforeseen circumstances, such as a fire or flood;

(f) deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

(g) 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

5.4.2. ANCBC Workers must immediately notify the ANCBC Data Protection Lead if they suspect that a breach has occurred or discover a breach.

5.4.3. ANCBC will:

(a) Take data breaches seriously; and

(b) make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 24 hours of becoming aware of it, <u>if it is likely to result in a risk to the rights and freedoms of individuals</u>; and

(c) notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
(See Appendix IV: Emergency protocols)

5.5. International Transfers

5.5.1. ANCBC and the Churches may only transfer personal data outside the European Economic Area where satisfied the organisation receiving the data has provided adequate safeguards by way of binding corporate rules or standard data protection clauses or compliance with an approved code of conduct.

5.6. Individual rights

5.6.1. All data subjects (including ANCBC Workers) have the following rights in relation to their personal data:

(a) to be informed about how, why and on what basis that data is processed;

(b) to obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request;

(c) to have data corrected if it is inaccurate or incomplete;

(d) to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten’);

(e) to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but they do not want the data to be erased); and

(f) to restrict the processing of personal data temporarily where they do not think it is accurate (and where ANCBC is verifying whether it is accurate), or where they have objected to the processing (and ANCBC is considering whether its legitimate grounds override their interests).

5.6.2. However, these rights are not absolute and there may be legal reasons why, for example, your data must be retained even if you ask for it to be erased. If you wish to exercise any of the rights in Section 5.6.1 please contact your Church Data Protection Lead and the ANCBC Data Protection Lead.

5.7. <u>ANCBC Data Protection Lead</u>

5.7.1. The Directors of ANCBC (the Board of Trustees) (the “**Trustees**”) have appointed Rickey Raja as ANCBC’s Data Protection Lead.

5.7.2. ANCBC’s Data Protection Lead is the owner of this Policy and has responsibility:

(a) to be familiar with relevant data protection legislation and regulations as far as they concern the charity and also church life and to respond to queries from the Church Data Protection Leads or the Trustees in relation to such legislation and regulations;

(b) to regularly review this Policy and if any changes are required obtain sign off from the Trustees;

(c) to ensure that each Church has a Data Protection Lead appointed who owns the day-to-day implementation of the arrangements outlined in this Policy for their Church;

(d) to request regular confirmation (preferably once a year) from each Church Data Protection Lead that they are performing their responsibilities as set out in Section 5.8.3 below;

(e) <u>to report any data protection concerns to the Trustees (including any potential data breaches) as soon as reasonably practicable;</u>

(f) if a data breach has occurred (see Section 5.4 above) determine (in conjunction with the Trustees) if such data breach is likely to result in a risk to the rights and freedoms of the individual concerned and if so, to make the required report to the Information Commissioner’s Office within 72 hours of becoming aware of such breach;

(g) if a data breach has occurred determine (in conjunction with the Trustees) if such data breach is likely to result in a high risk to the rights and freedoms of the individual concerned and, if so, then notify the affected individual;

(h) if an individual:

(i) requests information from ANCBC or a Church regarding how and why their data is being processed,

(ii) objects to any processing of their data by ANCBC or a Church, or

(iii) requests ANCBC or a Church to erase or rectify their data in any way,

to consult with all relevant persons to ensure that appropriate actions are taken in the required time frames;

(i) to request each Church Data Protection Lead to perform a data audit in relation to their Church at least every 2 years (or whenever else they deem necessary);

(j) to notify all ANCBC employees that they are required to have read and understood this Policy and ANCBC's Privacy Policy (and any updates); and

(k) to remind (preferably once a year) each Church Data Protection Lead that all Church volunteers (who process personal data on behalf of their Church) are required to have read and understood this Policy and ANCBC's Privacy Policy (and any updates).

5.8. <u>Church Data Protection Leads</u>

5.8.1. Each Church Senior Pastor (in conjunction with their Church Elders) has been given the responsibility by the Trustees to appoint a Data Protection Lead for their Church.

5.8.2. The current Church Data Protection Leads is Rickey Raja

5.8.3. The Church Data Protection Leads' responsibilities include:

(a) ensuring that the current ANCBC Privacy Policy is published on all Church websites and is included within any Church management system and as a link on Church email footers;

(b) ensuring, in relation to the Church and its activities, that a privacy notice (with a link to the ANCBC Privacy Policy) is provided to individuals at the point of any personal data collection (e.g. when they fill out an online form or a welcome card). Example wording is provided in ***Appendix III*** and if the Church Data Protection Lead is not certain as to which wording should be used they should consult the ANCBC Data Protection Lead;

(c) reporting any data protection concerns (including any potential data breaches) to the ANCBC Data Protection Lead or to a Trustee as soon as possible;

(d) if an individual:

(i) requests information from the Church regarding how and why their data is being processed,

(ii) objects to any processing of their data by the Church, or

(iii) requests the Church to erase or rectify their data in any way,

consulting with the ANCBC Church Data Protection Lead to ensure that appropriate actions are taken in the required time frames;

(e) ensuring that Church volunteers who process personal data on behalf of their Church have been provided with a copy of this Policy and ANCBC's Privacy Policy (and any updates) and have confirmed that they have read and understood the policies;

(f) performing a data protection audit in relation to their Church when requested by ANCBC's Data Protection Lead;

(g) ensuring that their Church does not enter into any agreements with an external organisation allowing such external organisation to process personal data on its behalf without obtaining sign off from

ANCBC's Data Protection Lead (to ensure that the external organisation is GDPR compliant and that sufficient safeguards are agreed in writing – e.g. the organisation will assist ANCBC in meeting its obligations in relation to the security of processing, notification of data breaches, return/deletion of personal data, subject access etc.); and

(h) ensuring that all ANCBC Workers who process personal data in relation to their Church work have been provided with adequate training about their data protection and information security responsibilities.

5.9. <u>Responsibility of ANCBC Workers in relation to personal data</u>

5.9.1. Those ANCBC Workers who have access to personal data in the course of their work must:

(a) be familiar with this Policy and ANCBC's Privacy Policy (a copy of which can be found on each Church website) and comply with their terms;

(b) only process personal data in accordance with the principles and requirements set out above (especially those in sections 5.1 to 5.4), and where they have overall responsibility for any personal data, must determine, document and review the lawful basis for processing that data in accordance with this Policy;

(c) only access the personal data that they have authority to access, and only for authorised purposes;

(d) only allow other ANCBC Workers to access personal data if it is necessary and if they have appropriate authorisation;

(e) keep personal data secure by complying with the rules on access to premises, computer access, password protection and secure file storage and destruction as set out Section 6 below;

(f) not remove personal data or devices containing personal data (or which can be used to access it) from the relevant Church/ANCBC premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the data on the device;

(g) not store personal data on local hard drives;

(h) not keep ANCBC/Church data for longer than is necessary in accordance with ANCBC's data retention periods (see Section 7 below and
Appendix I for the relevant retention periods – if it is unclear then the Church or ANCBC Data Protection Lead should be consulted);

(i) attend any data protection training they are invited to unless otherwise agreed by their Church Data Protection Lead or the ANCBC Data Protection Lead;

(j) immediately inform their Church Data Protection Lead and the ANCBC Data Protection Lead if an individual:

    (i) requests information from them regarding how and why their data is being processed,

    (ii) objects to any processing of their data, or

    (iii) requests to have their data erased or rectified in any way

(to ensure ANCBC meets its data protection obligations to those individuals in the required time frames);

(k) immediately contact their Church Data Protection Lead and ANCBC's Data Protection Lead if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

(i) processing of personal data without a lawful basis for processing and, in the case of sensitive personal data, without one of the special conditions in Section 5.3.3(b) also being met;

(ii) any data breach e.g. loss/theft of data, unauthorised access to personal data, accidental deletion/alteration of data, deliberate attacks on IT systems (see Section 5.4.1 above);

(iii) access to personal data without the proper authorisation;

(iv) removal of personal data, or devices containing personal data (or which can be used to access it) from ANCBC/Church premises without appropriate security measures being in place;

(v) any other breach of this Policy or any of the data protection principles set out in Section 5.1.1 above.

5.9.2. Those ANCBC Workers who assist with the recruitment of ANCBC Workers must ensure that during any recruitment process:

(a) no irrelevant questions are asked during the short-listing, interview and decision-making stages relating to sensitive personal data e.g. information relating to race or ethnic origin or health;

(b) if an applicant provides irrelevant sensitive personal data (e.g. the applicant provides it without being asked in his/her CV or during an interview) that no record is kept of such data and any reference to it is immediately deleted or redacted;

(c) 'right to work' checks are carried out before an offer of employment is made unconditional but not during the earlier short-listing, interview or recruitment decision making process.

6. Information Security

6.1. General

6.1.1. All ANCBC Workers who process personal data or other confidential information have a responsibility to:

(a) protect all personal data and other confidential information from loss, theft, misuse or inappropriate access or disclosure;

(b) discuss with line managers and their Church Data Protection Lead the appropriate security arrangements for the type of information they access in the course of their work;

(c) ensure they attend any data protection and/or information security training they are invited to unless otherwise agreed by their Church Data Protection Lead or the ANCBC Data Protection Lead;

(d) only use ANCBC/Church information in connection with work being carried out for ANCBC/their Church and not for personal purposes;

(e) ensure that all confidential information (including personal data) that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as the need for its retention has passed (see ***Appendix I*** for the relevant retention periods – if it is unclear then the Church or ANCBC Data Protection Lead should be consulted).

6.2. Human resources information

6.2.1. Given the internal confidentiality of personnel files, access to such information is limited to ANCBC's Director of Charity Services. Except as provided in individual roles, other ANCBC Workers are not authorised to access that information.

6.2.2. Any staff member in a management or supervisory role must keep personnel information confidential.

6.2.3. Staff may ask to see their personnel files in accordance with the relevant provisions of data protection legislation or regulations.

6.3. Access to offices and information

6.3.1. Where possible, office doors must be kept secure at all times and visitors should not be given keys or access codes. Where offices are also used for other purposes (e.g. as ministry venues) appropriate precautions should be taken to safeguard confidential information.

6.3.2. Documents containing personal data or other confidential information and equipment displaying personal data or other confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows.

6.3.3. Visitors should be accompanied at all times and never be left alone in areas where they could have access to personal data or other confidential information.

6.3.4. If it is necessary for a ANCBC Worker or a Church volunteer to meet with visitors in an office or other room which contains personal data or other confidential information, then steps should be taken to ensure that no such information is visible.

6.3.5. At the end of each day, or when desks are unoccupied, all paper documents and devices containing personal data or other confidential information must be securely locked away.

6.4. Computers and IT

6.4.1. Computers and other electronic devices (e.g. mobile phones or tablets) upon which a ANCBC Worker may access personal data or other confidential information must be password protected and single sign-ons (e.g. as offered by Google) should be avoided. Passwords should not be written down or given to others.

6.4.2. It is recommended that you:

(a) create different passwords for every account;

(b) make your passwords at least 15 characters long and that you use upper and lower case letters and include numbers and symbols;

(c) never use information in your password that can easily be found online, like your date of birth or recovery questions;

(d) do not store passwords on your computer, phone or tablet (many devices will back up your data to your cloud account and if your cloud account is hacked cyber criminals will have access to all the passwords that you have saved to the device);

(e) never save passwords when prompted by your browser but rather enter your username and password every time you visit the site;

(f) consider using a ‘pass phrase’ with a strong combination of upper and lower case letters, numbers and symbols as this will be easier to remember.

6.4.3. Computers and other electronic devices upon which a ANCBC Worker may access personal data or other confidential information should be locked when not in use to minimise the risk of accidental loss or disclosure.

6.4.4. Personal data and other confidential information must not be copied onto any removable hard drive, CD or DVD or memory stick / thumb drive without the express permission of the relevant Church Data Protection Lead and even then it needs to be password protected or encrypted. Personal information and other confidential information copied onto any of these devices should be deleted as soon as possible and stored on ANCBC’s or a Church’s computer network in order for it to be backed up.

6.4.5. ANCBC Workers should ensure they do not introduce viruses or malicious code onto ANCBC or Church systems. Software should not be installed or downloaded from the internet without it first being virus checked. ANCBC Workers should contact their Church IT lead for guidance on appropriate steps to be taken to ensure compliance.

6.4.6. Church volunteers who process personal data on behalf of a Church should, where reasonably practicable, be provided with a Church email address (e.g. safeguarding@ancbc.org). The relevant Church Data Protection Lead should be consulted in this regard.

6.4.7. Documents containing personal data and other confidential information should be stored within the ANCBC or relevant Church (cloud based) network (Sharepoint or Google Drive) or on Dropbox (e.g. where a Church volunteer does not have access to the ANCBC or Church network) and should always be password protected and access restricted

6.5. Communication

6.5.1. ANCBC Workers should be careful about maintaining confidentiality when speaking in public places.

6.5.2. Personal data and other confidential information should be circulated only to those who need to know the information in the course of their ANCBC or Church work.

6.5.3. When personal data or other confidential information needs to be removed from the relevant ANCBC or Church offices, all reasonable steps must be taken to ensure that the integrity of the information and that confidentiality is maintained. ANCBC Workers must ensure that personal data or other confidential information is:

(a) not transported in see-through or other un-secured bags or cases;

(b) not read in public places (e.g. waiting rooms, cafes, trains); and

(c) not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

6.5.4. Postal and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

6.5.5. When sending emails to multiple recipients the email addresses should be included as a blind carbon copy (“bcc”).

6.5.6. All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

6.6. <u>Home working</u>

6.6.1. ANCBC Workers should only take personal data or other confidential information home if appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information (if they have any doubts in this regard they should contact their Church Data Protection Lead or the ANCBC Data Protection Lead). In particular they must ensure that:

(a) any personal data or other confidential information is kept in a secure and locked environment where it cannot be accessed by family members or visitors;

(b) all personal data or other confidential information that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed; and

(c) if they access personal data or other confidential information via a shared family computer, that they have a separate password protected log-on which cannot be accessed by family members or visitors.

7. Retention of data

7.1. Data and records should not be kept for longer than is necessary. This principle finds statutory form in the Data Protection Legislation, which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose". Information should not be kept indefinitely unless there are specific requirements. **Appendix I** gives guidelines on timescales for the retention of various types of information.

7.2. When data is no longer required it should be appropriately destroyed (i.e. shredded or burnt and deleted from your local hard drive). If there is any uncertainty then the relevant Church or ANCBC Data Protection Lead should be consulted.

8. Questions on this Policy

8.1 If you have any questions or concerns about anything in this Policy, do not hesitate to contact the ANCBC Data Protection Lead.

Appendix I: Retention Period Guidelines

If you have any queries regarding retaining or disposing of data please contact your Church Data Protection Lead.

Types of Data	Suggested Retention Period
Information relating to children *NB. Please see the following article:* https://christiansafeguardingservices.phasic-ltd.co.uk/record-retention	• Check for accuracy once a year • Record that child was a member of the group - permanent • Secure destruction of personal data other than name and fact of membership - three years after cease to be a member
Church member information	• Check for accuracy once a year • Record that adult was a member - permanent • Secure destruction of personal data other than name and fact of membership - three years after cease to be a member
Church group member information	• Check for accuracy once a year • Record that adult was a member of group - permanent • Secure destruction of personal data other than name and fact of membership - three years after cease to be a member
Accident books, and records and reports of accidents	• (for Adults) 4 years after the date of the last entry • (for children) four years after the child attains 18 years (RIDDOR 1985)
Wages and salary records	• 6 years from the tax year in which generated
Income Tax and NI returns, including correspondence with tax office	• At least 6 years after the end of the financial year to which the records relate
Health records	• 12 months from date of leaving employment • (Management of Health and Safety at Work Regulations)
Health records where reason for termination of employment is connected with health, including stress related illness	• 4 years from date of leaving employment • (Limitation period for personal injury claims)

Types of Data (continued)	Suggested Retention Period
Personnel files (staff and volunteers) including: - training records - notes of disciplinary - grievance hearings.	• 7 years from the end of employment/ volunteering
Application forms / interview notes	• Maximum of one year from the date of the conclusion of the recruitment process. • If employed, retain in personnel file.

Appendix II: ANCBC's Personal Data Processing examples

Notes:

- Personal information should not be retained for any longer than is necessary. The length of time data should be retained will depend on the circumstances, including the reasons why the personal information was obtained. ANCBC Workers who process personal information should only retain personal information for the appropriate retention periods.
- Personal information that is no longer required should be deleted permanently from information systems and any hard copies should be securely destroyed (e.g. shredding)
- Below are some examples from regular church life:

Description (and sensitivity if applicable)	Serving rotas
Why the data can be held and for what uses	For rota administration purposes
Basis/bases for processing the data	Legitimate interest
Who can process the data, where it may be held, who can be allowed access to the data	Rota leaders/administrator – rota team members can also see the information.
Minimum security controls required	If possible this information should be accessed via a secure church management system (e.g. ChurchSuite). If rotas are printed out and put up on notice boards these should include only first names (and first letter of surname if there are two or more people with the same name)
How long the data should be kept for - data retention period	Information should be deleted by the latest 6 months after the rota has finished.

Description (and sensitivity if applicable)	Children's Sunday School Registers (NB. may include sensitive personal information e.g. health information)
Why the data can be held and for what uses	For Sunday School administration purposes, for safeguarding controls and for health and safety purposes (to record allergies, to be able to contact parents/guardians in the event of an emergency etc.)
Basis/bases for processing the data	Legitimate interest (and in relation to sensitive personal data either because ANCBC falls within Article 9(2)(d) GDPR or because of explicit consent)
Who can process the data, where it may be held, who can be allowed access to the data	Sunday School rota overseers, Sunday School leaders, staff, safeguarding leads

Minimum security controls required	If possible this information should be accessed via a secure church management system (e.g. ChurchSuite). If paper registers are used these should be held securely in a locked cabinet.
How long the data should be kept for – data retention period	Names and record of attendance to be stored indefinitely – for safeguarding purposes. Secure destruction of personal data other than name and fact of membership – three years after child ceases to be a member

Description (and sensitivity if applicable)	Event sign-ups for members and visitors (<u>may include sensitive personal information e.g. health information/dietary information</u>) e.g. Church dinners, Children's holiday clubs etc.
Why the data can be held and for what uses	For event administration purposes
Basis/bases for processing the data	Legitimate interest and/or legal obligation (and in relation to sensitive personal data either because ANCBC falls within Article 9(2)(d) GDPR or because of explicit consent) – event sign up form needs to have a link to the privacy policy if possible and should include details on how the data will be used– ***see Appendix III (example 5)*** **for example wording**
Who can process the data, where it may be held, who can be allowed access to the data	Event organisers and helpers, staff
Minimum security controls required	If possible event sign ups should be done online (either via Church management system such as ChurchSuite) or third party booking service provider (e.g. Eventbrite) which is GDPR compliant. Sign up via email is to be avoided but if necessary the sign ups should be to a generic Church email address and not a personal email address of a volunteer
How long the data should be kept for – data retention period	Data relating to adults should be deleted within 6 months after the event occurred (unless there is a specific reason to retain the information e.g. to provide information about future related events) However, names and record of attendance of all children to be stored indefinitely – for safeguarding purposes.

Description (and sensitivity if applicable)	Safeguarding application forms, ID checks and notes on safeguarding issues (<u>may include information regarding criminal convictions/ offences or sensitive personal data</u>)

Why the data can be held and for what uses	For safeguarding administration/compliance purposes
Basis/bases for processing the data	Consent: those persons who apply for a DBS check through ANCBC are required to consent to providing personal information (including sensitive personal information relating to any criminal convictions they may have) in order for ANCBC to fulfil its safeguarding best practice process and/or legal obligation
Who can process the data, where it may be held, who can be allowed access to the data	The Safeguarding Co-ordinator, safeguarding reps, pastors and children's leaders
Minimum security controls required	Internal Church safeguarding forms to be processed via Cognito Forms (forms are encrypted and Cognito Forms has signed up to the EU-US Privacy Shield) Applicants currently apply directly for their DBS via CCPAS and only the Safeguarding and Compliance Co-ordinator has access to notes on a DBS Church safeguarding administrators who process personal data should never send this data via a personal email account Any spreadsheets which contain safeguarding information should be password protected and should be stored on a Church information system or on Dropbox (with limited access) ID checks – CCPAS registered ID checkers should try to do all ID checks online with the applicant so that no photocopies of passports etc. are taken. If this is not reasonably practicable the ID checker should request permission to take a photocopy and advise that they will shred the documents when the ID check has been processed (and also confirm with the applicant when this has been done). Taking photos (on mobile phones) of ID documents should be avoided if at all possible – and should only ever be done with the applicant's consent (and the ID processor should confirm that the image has been deleted as soon as the ID check has been processed). If a safeguarding concern is raised this should be dealt with by Safeguarding and Compliance Co-ordinator – if an email needs to be sent (to be avoided where possible) pseudonymisation of names should be used
How long the data should be kept for - data retention period	Indefinitely

Description (and sensitivity if applicable)	Pastoral notes (<u>may include sensitive personal data</u>)

Why the data can be held and for what uses	To provide pastoral support
Basis/bases for processing the data	Legitimate interest (and in relation to sensitive personal data because ANCBC falls within Article 9(2)(d) GDPR) if the person is a regular member, there are sufficient security controls in place and the information is not disclosed outside of ANCBC/ the Churches (and access to information is restricted to only those staff/Elders who need to know the information) ***see Appendix III (example 3 for example privacy notice wording)***
Who can process the data, where it may be held, who can be allowed access to the data	Church pastors and other senior staff who may be required to know the information (e.g. the Safeguarding and Compliance Co-ordinator)
Minimum security controls required	Paper notes should be kept in a secure locked cabinet and pseudonyms should be used where possible. Emails should be avoided where at all possible and if an email needs to be sent, pseudonyms should be used
How long the data should be kept for – data retention period	Generally, these should be destroyed as soon as possible. Some may need to be held indefinitely, but if pastoral issue dealt with or person leaves church, data should be erased after an appropriate period – to be determined on a case by case basis.

Description (and sensitivity if applicable)	Congregation lists / Church directory (on a Church management system such as ChurchSuite or where the size of the congregation is too small to warrant a church management system, in a spreadsheet or printed on paper)
Why the data can be held and for what uses	**Purpose 1** For communication with members of congregations by ANCBC Workers only (and NOT shared with wider church families) OR **Purpose 2** In addition to the above, for church members to contact one another NB. newcomers, guests and visitor details should NOT ever be visible to anybody other than Church Workers until they take the decision (and they may never) to commit to joining the church (demonstrated for example, by joining a small group). Should they reach that point, they need to be clearly told that their data will be seen by their church family and how to control and limit its visibility.

Basis/bases for processing the data	**Purpose 1** Legitimate interest – staff communication with members; **Purpose 2** Legitimate interest of organisation (building-up the church family) and legitimate interest of members to be able to communicate together, serve and support one another
Who can process the data, where it may be held, who can be allowed access to the data	**Purpose 1** Church staff and approved volunteers ONLY will have access to the data **Purpose 2** Church members or regulars will have access via a log-in which will only be granted to them when approved by the appropriate Church Worker. Users must be given a Privacy Notice which explains that other members of the church will be able to see their details; be able to control which details are made visible; and be able to request (through a simple, clear process) any or all details be removed.
Minimum security controls required	ChurchSuite is GDPR compliant and members access by means of password – using a church management system avoids people having paper copies with members' personal details. Paper church directories should be avoided where possible. However, if necessary, then the paper directory should be marked Confidential and should include instructions about safe storage of the directory.

How long the data should be kept for – data retention period	As long as the person is a member of a congregation. If they leave, then they will be given the opportunity to remain on the Church database (to only be accessed by staff) so that we can keep them updated on certain selected news that we think they might be interested in (they can ask to be removed from the alumni list at any time and if an email is sent to them the email should indicate that they can ask to be removed from the alumni list upon request). If a person confirms they have left a congregation and/or we have not heard or seen them for a period of 6 months they should be archived within the relevant Church database and their details should be deleted at the latest 1 year after being archived. In relation to any paper church directory their details should not be included in any future church directory. Specific information will also be removed from a directory (future copies if in paper form) if individual concerned requests – individual can manage this themselves on ChurchSuite.

Description (and sensitivity if applicable)	Visitor lists
Why the data can be held and for what uses	To be able to welcome newcomers and provide them with information we think is relevant to them
Basis/bases for processing the data	Consent – visitors will only be included on a Church database if they provide their contact details on a welcome card **(see *Appendix III* example 1 for example wording)** Legitimate interest – to enable welcome teams and staff to effectively welcome newcomers
Who can process the data, where it may be held, who can be allowed access to the data	Welcome team members and Church Workers
Minimum security controls required	If a welcome book is used this should be securely locked away after use by the welcome team. Names etc. of newcomers should only be included within a secure Church database or in a secure file (e.g. in DropBox) with only the relevant welcome team having access to the information. There should be passwords to protect the information and no personal information should be emailed from personal email addresses.

How long the data should be kept for - data retention period	If the visitor becomes a regular and joins a Bible study group their information will be kept until they leave the congregation (see above) If the visitor is not seen or heard from for a period of 6 months their personal data should be deleted/redacted at the latest 1 year after they were last seen/heard from.

Description (and sensitivity if applicable)	Training registers e.g. safeguarding training, health and safety training, data protection training
Why the data can be held and for what uses	To show compliance with laws/regulations
Basis/bases for processing the data	Legitimate interest and/or legal obligation
Who can process the data, where it may be held, who can be allowed access to the data	The person/s responsible for policy implementations
Minimum security controls required	Paper records kept in a locked cabinet and where possible paper records destroyed and digital records kept within a secure Church database
How long the data should be kept for - data retention period	Indefinitely to be able to show compliance

Description (and sensitivity if applicable)	Personnel records (<u>including sensitive personal information about health</u>)
Why the data can be held and for what uses	For staff administration (including e.g. processing salary payments, keeping sickness absence records, monitoring staff attendance)
Basis/bases for processing the data	Legitimate interest, in the proper management of the working relationship; contract (and in relation to sensitive personal data either because ANCBC falls within Article 9(2)(d) GDPR or Article 9(2)(h) GDPR applies or because of explicit consent) ***see Appendix III (example 7) for example wording***
Who can process the data, where it may be held, who can be allowed access to the data	Charities services team, stewardship payroll once established.
Minimum security controls required	All paper records kept in locked cabinet, payroll provider and auditors GDPR compliant
How long the data should be kept for - data retention period	7 years after employment ceases

Description (and sensitivity if applicable)	Rejected job applicant records (including application letters/CVs/references/interview notes etc.)
Why the data can be held and for what uses	
Basis/bases for processing the data	
Who can process the data, where it may be held, who can be allowed access to the data	
Minimum security controls required	Paper records must be kept in locked cabinet
How long the data should be kept for - data retention period	12 months after conclusion of the recruitment process

Description (and sensitivity if applicable)	Emailed newsletters containing Church news
Why the data can be held and for what uses	To provide Church members and/or visitors and/or other interested parties with relevant information
Basis/bases for processing the data	Consent – for those who are not Church members (needs to be explicit opt in consent e.g. via welcome card – **see *Appendix III* example 1 for example wording**) Consent – required for fundraising or promotional emails (except those that are sent by post) Legitimate interest – for Church members if the email/newsletter contains information that they would reasonably need to be aware of as a member of a Church and will help them get the most out of church life, but they should be able to opt out of receiving these at any time (include privacy wording and link to Privacy Policy)
Who can process the data, where it may be held, who can be allowed access to the data	Church administrators, Ministry leaders, staff
Minimum security controls required	Where possible sent via Church management system but if not sent via a Church email address (not a personal email address). Emails should never show other recipient information (i.e. email addresses of others) and recipients should be included as "bcc"
How long the data should be kept for - data retention period	Until request for deletion, archived after [2] years

Description (and sensitivity if applicable)	Feedback and help forms

Why the data can be held and for what uses	To allow members and visitors to ask for help or give feedback and to enable us to respond
Basis/bases for processing the data	Legitimate interest
Who can process the data, where it may be held, who can be allowed access to the data	Church administrators, staff
Minimum security controls required	
How long the data should be kept for - data retention period	To be determined on a case by case basis or until request for deletion (refer to Church Data Protection Lead for advice)

Description (and sensitivity if applicable)	Photographs (<u>may be sensitive personal data as it could be seen as suggestive of religious beliefs, and/or indicate race/ethnicity</u>)
Why the data can be held and for what uses	To be used as an internal record of events or congregation members; or to be used on websites/ newsletter etc.
Basis/bases for processing the data	Legitimate interest – if going to be used for internal purposes Consent – if persons can clearly be identified in a photograph and the photo is going to be used on website/newsletter etc. **(see example wording in example 2, *Appendix III*).**
Who can process the data, where it may be held, who can be allowed access to the data	Church administrators, staff
Minimum security controls required	Copies of photos should be held on a secure Church server and only used externally (e.g. on website) if we have the relevant consents on file (see ***Appendix III*** for an example consent form). Even with consent names of children and young people should not to be published alongside their photographs.
How long the data should be kept for - data retention period	To be determined on a case by case basis in consultation with the Church Data Protection Lead.

Description (and sensitivity if applicable)	Gift Aid Declarations
Why the data can be held and for what uses	For claiming gift aid
Basis/bases for processing the data	Consent – by completing of declaration; and legal obligation

Who can process the data, where it may be held, who can be allowed access to the data	Church treasurer/s and ANCBC's Gift Aid Officer/ Finance Officer
Minimum security controls required	Paper forms must be kept in a locked filing cabinet or secure office
How long the data should be kept for - data retention period	6 years after last gift claimed on the declaration

Appendix III: Privacy notice examples

(to be read with Appendix II above)

Privacy notices should also be provided to individuals at the point of personal data collection (e.g. when they fill out an online form) to explain the purpose for which their data is being collected. This is important because we cannot normally collect data for one purpose and then use it for another purpose. The following example privacy notices should be amended/adapted depending on the purpose for which the data is being collected. If you require help in this regard, please contact your Church Data Protection Lead or the ANCBC Data Protection Lead.

1. WELCOME CARD EXAMPLE

We hope you've enjoyed being with us today! We would like to get to know you and to tell you more about our church and so please complete this card and let us know how we may contact you.

Name(s) ______________________________

Address: ______________________________

____

Email: ______________________________

Phone(s): ______________________________

Names and ages of any children

____

By completing this form, I/we consent to All Nations Church Barkingside & Clayhall holding this information to keep me/us informed about All Nations Church news, events, activities and opportunities to participate in church life.

Tell me more!

- ☐ Youth and kids
- ☐ Exploring Christianity
- ☐ News and Events
- ☐ Newcomers group

I would also like to know…?

I/we consent to All Nations Church Barkingside & Clayhall contacting me by

▫ email ▫ phone ▫ post ▫ text ▫ social media

All Nations Church Barkingside & Clayhall is part of the Co-Mission network of Church and FIEC and we take privacy very seriously. Your information will be stored on our secure online database and will only be seen by church staff, leaders and volunteers who have been approved by us. We do not share your information with third parties unless the law requires us to do so and you can find out more by reading our Privacy Policy which is available on our website or from the church office. If at any time you wish to stop receiving communications from us, or want to withdraw or change your consents, please contact the Church administrator at info@ancbc.org.

Welcome card example - explanatory comments

When communicating with church members / regulars, we will generally rely on "legitimate interest" as our lawful basis for processing personal data and we will not need to seek their specific consent. However, with visitors, guests and newcomers, we need to be particularly careful because they:

a. Have not yet made any commitment to our church and may be nervous about doing so;

b. May not be converted and we want to help them spiritually, not place unnecessary hurdles in their path;

c. May be sensitive to Privacy issues and be quick to make formal complaints.

Therefore, we would be wise to obtain their consent to holding their information and to contacting them in the future. As they are not yet part of the church, such communications would probably be viewed as being "direct marketing" and so consent will be especially important if we are contacting them electronically (see The Privacy and Electronic Communications Regulations (PECR) which sit alongside the Data Protection Act and the GDPR).

The formatting in the above welcome card is deliberately simple – churches will no doubt wish to personalise & brand and designers will soon be very familiar with the new tick box requirements!

Please note:

Marketing consents

We need to include separate tick boxes for all the methods of communication we may wish to use. If a newcomer only wants to receive emails from us, they must be able to say so when giving consent and we must respect their wishes by not trying to contact them any other way!

Limited consent

By completing this form, newcomers are consenting to their information being used for certain purposes. This does NOT give us the right to use that information for additional and/or different purposes! For example, the consent does allow the church to store their information electronically (e.g. on [ChurchSuite]) and allows staff, leaders and approved volunteers to view it. However, the consent does:

- NOT entitle everybody at the church to see this information. Therefore, other users of [ChurchSuite] must not be granted visibility of this information; and

- NOT allow the church to publish any of the information in any church address book or directory (paper or electronic); and

- NOT allow the church to include photographs of them (or from which they can be identified) on the church website or in any other literature.

2. PHOTOGRAPHY/FILMING CONSENT FORM EXAMPLE

Any photo/s or film taken [on the day] will be used by us both as a record [of the day] and for promotional purposes.

We may use any photo/s and/or film we take:

- on our website/s or social media;
- in email newsletters;
- in printed materials (such as leaflets, posters and adverts for public display); or
- in materials sent out to the media

It is important to note that websites and social media can be seen throughout the world and not just in the United Kingdom.

Our use of any photo/s or film will be subject to the following conditions:

- we will not use any photo/s or film for purposes than those mentioned above;
- we will not include your personal e-mail or postal addresses or telephone numbers on our website/s, social media or in printed publications but may include your name (but not the full names of any children) in connection with a photo or film.
- you waive any intellectual property rights that you may have in such photo/s and/or film and acknowledge that all right, title and ownership in and to such photo/s and/or film, including copyright, to the extent permitted by law, shall belong to us exclusively.

Please indicate below if you provide us with permission to take photo/s and/or film and that you agree we have the irrevocable right to use, publish, reproduce and display such photo/s and/or film for the purposes and in accordance with the conditions set out above:

YES ☐

NO ☐

Your Name	
Your Address	
Your telephone Number	
Your signature (by signing this form you are also confirming that you are over 18 years old)	
Date	

3. PASTORAL CARE PRIVACY NOTICE EXAMPLE WORDING

To enable us to provide adequate pastoral support to you and your family, the pastors, elders, trustees, staff team and safe-guarding co-ordinators and deputy and administrator of ANCBC may record information which may be regarded as sensitive. Unless we are legally obliged to do so, this information will NOT be disclosed to anyone else without your consent. For a full copy of our Privacy Policy please see www.ancbc.org

4. HOLIDAY CLUB / CHURCH YOUTH GROUP SIGN UP (WHERE SENSITIVE PERSONAL DATA MAY BE COLLECTED)

We are collecting this information to enable the church to plan and run the [insert name of holiday club/youth group] and to ensure your child's safety and security whilst at the [insert name of holiday club/youth group]. We will only contact you in case of an emergency and occasionally with important information regarding [insert name of holiday club/youth group] or events related to the [insert name of holiday club/youth group].

We will process this information mainly on the basis of our legitimate interests. However, in relation to any health or allergy information you provide, you will need to consent to us processing this data (please tick the relevant box below). If you do not consent, we will be unable to accept your child at the [insert name of holiday club/youth group] as this data is required to help us maintain our high standards of safety.

The personal data which you provide will be held by us for the duration of the academic year in which it is provided, following which we will review on a regular basis whether we need to continue to hold this data. Factors relevant to this review will include (i) whether your child is still in the [insert name of holiday club/youth group] age range; and (ii) whether your child is still regularly attending [insert name of holiday club/youth group].

Where there has been an incident at [insert name of holiday club/youth group] (such as an injury) involving your child, we may ask you to fill in a specific incident form at the end of the [insert name of holiday club/youth group] session in which the incident occurred. We will hold the information provided on this form on the basis of our legitimate interests and may hold this for longer than the personal data provided in other contexts.

We will seek to keep the personal data you have provided up to date and will usually request that a new form is filled out for each academic year to ensure that this is done.

Only [the Holiday Club leaders and the youth pastor/children's worker] will have access to this information. The forms will be destroyed once [insert name of holiday club/youth group] has finished unless you have ticked the box asking us to keep you informed about future activities we think your child might be interested in attending. If this is the case, we will retain your details for the sole purpose of notifying you of such events. We also have a legal obligation to retain a record of your child's attendance at holiday club/youth group.

For more information about your rights in respect of your and your child's personal data, and how we hold and process your and your child's personal data, please see our full Privacy Policy, which can be found here.

5. EVENT SIGN UP (WHERE SENSITIVE PERSONAL DATA MAY BE COLLECTED)

We are collecting this information to enable the church to plan and run the [insert name] event and to ensure your [and/or your child's] safety and security whilst at the event. We will only contact you in the case of an emergency or with important information regarding the event.

We will process this information mainly on the basis of pursuing our legitimate interests. However, in relation to any health or allergy information you provide, you will need to consent to us processing such data (please tick the relevant box below). If you do not consent, we will be unable to accept your [and/or your child's] booking onto the event as this data is required to help us maintain our high standards of safety. Please contact us if you wish to withdraw your consent, or if you have any other queries about how we hold your data.

Only [the event leaders, event helpers and Church staff] will have access to this information. The forms will be destroyed within 6 months of the event taking place unless you have ticked the relevant box below asking us to keep you informed about future events we think you [or your child] might be interested in attending. If this is the case, we will retain your details for the sole purpose of notifying you of such events. A record will also be kept of those who attended this event.

For more information about your rights in respect of your [and your child's personal data], and how we hold and process your [and your child's personal data], please see our full Privacy Policy, which can be found here.

6. EMAIL FOOTER PRIVACY NOTICE WORDING

All Nations Church Barkingside & Clayhall is part of the Co-Mission Network of churches and the FIEC. Click **here** to view our Privacy Policy.

7. EMPLOYMENT APPLICATION FORMS

The personal data you provide in your application and as part of the recruitment process will only be held and processed for the purpose of selection processes and in connection with any subsequent employment or placement, unless otherwise indicated. Your data will be retained only for as long as is permitted by UK legislation and then destroyed. For a full copy of our Privacy Policy please see www.ancbc.org.

Appendix IV: Emergency protocols

The GDPR require organisations to respond urgently in certain situations. Such action can be difficult for charities with limited staff resources and with trustees who are key decision makers, but are also volunteers and busy people often employed by third parties. The protocols below show what action ANCBC will take, who will be involved and the timescales required in such emergency situations.

1. Data breach

1.1. ANCBC holds and processes personal data which needs to be protected. Every care is taken to protect the data we hold. Compromise of information, confidentiality, integrity or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance and financial penalties. We must contain any breaches, minimise the risks associated with the breach and consider what action is necessary to secure personal data and prevent any further breach.

1.2. An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to data subjects. An incident includes but is not restricted to:

- 1.2.1. Loss or theft of personal data or the equipment on which the data is stored e.g. laptop, memory stick, smartphone, or paper record
- 1.2.2. theft or failure of equipment on which personal data is stored
- 1.2.3. Unauthorised use of or access to personal data
- 1.2.4. Attempts to gain unauthorised access to personal data
- 1.2.5. Unauthorised disclosure of personal data
- 1.2.6. Website defacement
- 1.2.7. Hacking attack

1.3. As soon as an employee, worker or volunteer discovers that there has been, or has grounds to suspect that there may have been, a Data breach (see 5.4 of Policy), they must immediately contact the ANCBC Data Protection Lead Rickey Raja. The ANCBC Data Protection Lead will then notify the Trustees as soon as reasonably practicable.

1.4. If the ANCBC Data Protection Lead is not contactable (for example, on holiday), then the report should be made immediately to one of the Trustees.

1.5. The initial report to the ANCBC Data Protection Lead and/or Trustees (under 1.3 or 1.4 above) should contain the following details:

- 1.5.1. Date and time of discovery of breach
- 1.5.2. Details of person who discovered the breach
- 1.5.3. The nature of the personal data involved
- 1.5.4. How many individuals' data is affected

1.6. On being informed of the probable or actual Data breach, the ANCBC Data Protection Lead or Trustee will first ascertain if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effects of the breach. They will then conduct an immediate investigation to ascertain what has happened, who has been affected and the potential severity of the breach.
An investigation will be carried out without delay and where possible within 24 hours of the breach being discovered. the ANCBC Data Protection Lead or Trustee will assess the risks associated with the breach, the potential consequences for the data subjects, how serious and substantial those are and how likely they are to occur.

1.7. The investigation will take into account the following:

1.7.1. The type of data involved and its sensitivity

1.7.2. The protections in place (e.g. encryption)

1.7.3. What has happened to the data

1.7.4. Whether the data could be put to illegal or inappropriate use

1.7.5. Who the data subjects are, how many are involved, and the potential effects on them

1.7.6. Any wider consequences

All those involved in the Data breach will be required to make themselves available to those involved in the investigation. Where criminality has occurred, the police will be notified.

1.8. The Trustees (in liaison with the ANCBC Data Protection Lead) will determine with appropriate advice who needs to be notified of the breach. Every incident will be assessed on a case by case basis. The Information Commissioner will be notified, if at all possible **within 24 hours of the data breach and at the latest, within 72 hours of becoming aware of such breach**, if a large number of people are affected or the consequences for the data subjects are very serious.

Guidance on when and how to notify the ICO is available on their website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

1.9. Where appropriate (if the Data breach is likely to result in a high risk to the rights and freedoms of the individual concerned), we will notify the data subjects whose personal data has been affected by the incident; such a notification may include a description of how and when the breach occurred, and the nature of the data involved, and specific and clear advice on what they can do to protect themselves and what has already been done to mitigate the risks.

1.10. The ANCBC Data Protection Lead will keep a record of all actions taken in respect of the breach.

1.11. To make their determinations (1.8 and 1.9 above), the Trustees may seek legal advice from ANCBC's solicitors.

1.12. The Trustees will also decide if they need to notify their insurers or make a Serious Incident Report to the Charity Commission (which would be drafted by

ANCBC's solicitors).

1.13. Once the incident is contained, The ANCBC Data Protection Lead will carry out a review of the causes of the breach, the effectiveness of the response, and whether any changes to systems, policies or procedures should be undertaken. Consideration will be given to whether any corrective action is necessary to minimise the risk of similar incidents occurring. He will then report to the Trustees accordingly.

2. Subject Access Request

2.1. A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under Article 15 of the GDPR (formerly section 7 of the Data Protection Act 1998 (DPA)). The request does not have to be in any particular form. Nor does it have to include the words 'subject access' or make any reference to the DPA or GDPR. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act (FOIA).

2.2. In most cases we must respond to a SAR promptly and in any event **within 1 calendar month of receiving it.** It may be possible to extend this by up to two months in limited circumstances.

2.3. If an employee, worker or volunteer receives, or suspects he has received, a SAR, he must immediately notify his respective Church Data Protection Lead and also the ANCBC Data Protection Lead (see contact details above in 1.1 of this Appendix) or, where he is unavailable, to a Trustee (see contact details above in 1.2 of this Appendix).

2.4. When a SAR is received, the ANCBC Data Protection Lead and/or the Trustees will seek to act in accordance with the ICO's guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

They will act quickly, having regard to the 1 month deadline and will work with the Church Data Protection Lead and all appropriate employees, workers and volunteers to ascertain what personal data is held, how it is held, by whom it is held and for what purpose. They will put together their response, taking all reasonable efforts to ensure that the response is complete and accurate. Where the relevant data refers to other persons or to confidential matters, great care will be taken to ensure that the privacy of other persons is not breached and that confidentiality is maintained.

2.5. When preparing their response, the ANCBC Data Protection Lead and/or the Trustees may seek legal advice from ANCBC's solicitors.