Name of policy	GOV FOps - Data protection policy
Reviewed	Oct 2018
Update interval	Every three years
Authorised sign-off	Board of Trustees

BMS World Mission Data Protection Policy

1. POLICY STATEMENT

1.1 We (BMS World Mission) are committed to protecting personal data and respecting the rights of individuals whose personal data we collect and use. We are registered as a data controller with the Information Commissioner's Office (ICO) with registration number Z8899170 and process the personal information of individuals in the purpose of fulfilling the organisational objects.

We process personal data to enable us to, among other purposes:

1. Enable Baptist Churches to respond to the call of God throughout the world
2. Administer supporter records;
3. Fundraise and promote the interests of the charity;
4. Manage our employees, mission personnel and volunteers;
5. Maintain our own accounts and records;

1.2 Everyone has rights regarding the way in which their personal data is handled. In line with our values and aims, we are committed to good practice in the handling of personal and confidential information and to ensuring that such information is stored securely and is processed in accordance with the law.

2. PURPOSE OF THIS POLICY

2.1 This policy is designed to comply with relevant legislation including the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

2.2 In the course of our work, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, contractors who provide us with technical services or payment services).

2.3 We process the personal information of individuals in both electronic and paper form with all data protected under data protection law. In some cases, this will include sensitive information about individuals' religious or other beliefs, finances and personal circumstances. We also hold less sensitive information such as names and contact details, education and employment details, and visual images of current, past and prospective staff, mission personnel, volunteers, supporters, and contact details of advisers, complainants, enquirers, representatives of other

organisations as well as business and other contacts such as suppliers. We may also receive other personal information from the above or other sources.

2.4 We are aware that individuals can be harmed if their personal information is misused, is inaccurate, if it gets into the wrong hands as a result of poor security or if it is disclosed carelessly.

2.5 We are committed to protecting personal data and information from unauthorised disclosure and ensuring its accuracy. Breaches of data security or confidentiality are serious incidents. If they occur, they will be investigated fully and actively managed to ensure that any breach is as limited as possible. We may also be required to report breaches to the Information Commissioner's Office (ICO) if a breach results in a risk to an individual, and to inform the data subject if the breach results in a high risk to any person.

2.6 We recognise that all data subjects have a right to obtain from us copies of personal data which we hold about them.

3. DATA PROTECTION PRINCIPLES

3.1 BMS and contracted processors will comply with the GDPR's Principles. These provide that personal data must:

1. be processed lawfully, fairly and in a transparent manner (see section 4 below);
2. be processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;
3. be adequate, relevant and limited to what is necessary for the purpose;
4. be accurate and, where necessary, up to date;
5. not kept longer than necessary for the purpose, unless it is retained for public interest, scientific, historical research or statistical purposes and appropriate measures are taken to safeguard the rights of data subjects;
6. be processed in a manner which ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational means
7. be processed in accordance with the rights of data subjects (see section 10 and Schedule 1)
8. not be transferred (or stored) outside the European Union (EU) unless this is permitted by the GDPR (see section 15). This includes storage on a cloud the servers of which are located outside the EU

4. FAIR AND LAWFUL PROCESSING

4.1 Fairness of processing means that we will only process data in the manner in which data subjects reasonably expect. In order to make data subjects aware of how we

process personal data, the GDPR requires that we provide data subjects with certain information when we collect information from them as well as when we collect information about them from other sources.

4.2 If personal data is collected directly from data subjects, we will inform them (in writing) of the nature of the data collected and the relevant privacy notice.

4.3 If data is collected from a third party rather than directly from the data subjects, we will provide to the data subjects (in writing), within a reasonable time and not later than one month after we collect the data, with the relevant Privacy Notice and the nature of the data collected including

1. The categories of data concerned;
2. The source of the personal data

If we use personal data collected in this manner for communicating with data subjects BMS will provide this information not later than the time of our first communication with them, and if we intend on disclosing any of the personal data we must provide this information before the disclosure.

If we collect data from the data subject and we are aware that we will later be collecting additional data from third party sources, it may be more effective to provide all the information to the data subject when we collect the data from them.

LAWFUL PROCESSING

4.4 Processing of data is only lawful if at least one of the conditions listed in Article 6 of the GDPR is satisfied. The main conditions on which we rely are:

1. **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose
2. **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
3. **Legal obligation:** the processing is necessary for you to comply with the law
4. **Vital interests:** the processing is necessary to protect someone's life.
5. **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
6. **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. When we rely on the legitimate interests ground we will carry out a balancing exercise, weighing our legitimate interests with the rights of the individuals concerned

4.5 When sensitive personal data is processed, we will satisfy one of the conditions set out in Article 9 of the GDPR. These include:

1. The data subject has explicitly given consent;
2. The processing is necessary for carrying out our obligations under employment and social security and social protection law;
3. The processing is necessary for safeguarding the vital interests (in life or death situations) of an individual and the data subject is incapable of giving consent;
4. The processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
5. The processing is necessary for pursuing legal claims. The GDPR provides other alternatives for processing sensitive personal data as well and before deciding on which condition should be relied upon, the original text of the GDPR should be consulted together with any relevant guidance.

4.6 Other than in the specific circumstances described in section 4.7, information relating to criminal convictions and offences will not be processed unless the processing is authorised by law or is carried out under the control of official authority. This includes information about (i) allegations of criminal offences' (ii) proceedings in relation to criminal or alleged offences; and (iii) the disposal of criminal proceedings including sentencing. Sensitive personal data can only be processed under strict conditions, including the data subject's explicit consent (although other alternative conditions can apply in limited, very specific circumstances as described below).

4.7 Sensitive personal data may be processed for the purpose of safeguarding children or individuals at risk where it meets the substantial public interest condition under Schedule 1, Part 2 of the Data Protection Act 2018 and the processing is necessary for:

1. protecting an individual from neglect or physical, mental or emotional harm; or
2. protecting the physical, mental or emotional well-being of an individual where that individual is aged under 18 or aged 18 and over and at risk and if the circumstances so demand, may be without the explicit consent of the data subject where obtaining consent would prejudice the provision of protection for the child or individual at risk.

5. CONSENT

5.1 If consent is the basis of justifying processing it can be withdrawn at any time and if withdrawn, the processing will cease. Data subjects will be informed of their right to withdraw consent.

5.2 The GDPR requires consent to be a freely given, specific, informed and unambiguous indication of the data subject's wishes. It must be a statement or clear affirmative action which signifies agreement to the processing of personal data relating to the member. As a result, presumed consent and pre-selected opt-in boxes will not constitute valid consent under the GDPR.

6. PROCESSING FOR SPECIFIED PURPOSES

6.1 We will only process personal data for the specific purposes set out in our Privacy Notice or for other purposes specifically permitted by law. We will notify those purposes to the data subject in the manner described in section 4 unless there are lawful reasons for not doing so and this is permitted by a legal exemption.

6.2 We may process data for further purposes which we might not have envisaged when providing the data subject with the original privacy notice as long as the further purpose is compatible with the original purpose for which the data was collected. When assessing compatibility, we will consider, among all other relevant issues, the link between the purposes, the context in which the data was collected, the reasonable expectation of the data subject concerned, the nature of the personal data, the consequences of the further processing and the existence of appropriate safeguards. We are required to inform data subjects of the further purposes and provide them with appropriate additional information before we commence the further processing.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect and use personal data to the extent that it is required for the specific purpose described in section 6 (which would normally be notified to the data subject). We should collect and use just enough information, which is relevant, to achieve that purpose, but not more than is required.

7.2 We will check records regularly for missing information and to reduce the risk of irrelevant or excessive information being collected.

7.3 When implementing systems which involve processing personal data we will consider how such systems can provide for data minimisation by design and by default as described in section 18.

8. ACCURATE DATA

8.1 We will ensure that personal data held is accurate and kept up to date within an appropriate timescale.

9. DATA RETENTION AND DESTRUCTION

9.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected, and we will comply with relevant guidance

issued to our sector with regard to retention periods for specific items of personal data. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10. PROCESSING IN ACCORDANCE WITH DATA SUBJECTS' RIGHTS

10.1 We will process all personal data in line with data subjects' rights, in particular their right to:

1. Request access to any personal data held about them by us (the right of subject access is discussed in section 12 below),
2. Prevent the processing of their personal data for direct-marketing purposes (discussed in section 11 below);
3. Ask to have inaccurate personal data amended; and
4. Object to processing, in certain circumstances

11. DIRECT MARKETING

11.1 'Direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This includes contact made by organisations to individuals solely for the purposes of promoting their aims and the advertising need not be of a commercial product, nor need anything be offered for sale. BMS will adhere to the rules set out in the GDPR, the Privacy and Electronic Communications Regulations and any laws which may amend or replace the rules governing direct marketing when we make contact with data subjects, whether that contact is made by (but not limited to) post, email, text message, social media messaging, telephone (both live and recorded calls) and fax. Stricter rules apply to marketing by email and other electronic means including text messaging, social media messaging, fax and automated telephone calls.

11.2 Any direct marketing material that we send will identify us as the sender and will describe how an individual can object to receiving similar communications in the future.

11.3 Data subjects have a right to object to any form of processing of their personal data for a direct marketing purpose. If an individual exercises their right to object we will cease processing for this purpose within a reasonable time.

11.4 BMS is registered with the Fundraising Regulator and commits to adhering to the Fundraising Code of Practice (or any replacement code of practice).

12. SUBJECT ACCESS REQUESTS (SARs)

12.1 All data subjects have a right to obtain from us copies of personal data which we hold about them. Schedule 1 sets out the information that will be provided along with the methodology by which a request may be made.

12.2 We will not charge a fee for complying with a subject access request save in exceptional circumstances described in Schedule 1.

12.3 Except in limited circumstances when complying with a subject access request we will not disclose the personal data of third parties. For this reason, personal data of third parties will be redacted from documents which are provided to the requester.

12.4 In certain circumstances, exemptions may apply which may require or allow us to withhold information requested in response to a subject access request.

12.5 We will keep records of all subject access requests and a record of why information was redacted or withheld (e.g. subject to an exemption).

13. DISCLOSURES OF INFORMATION TO THIRD PARTIES (DATA SHARING)

13.1 All personal data is held securely by us and will be treated in a confidential manner. We will only disclose personal data when we have legal grounds to do so and if we have previously informed the data subject about the possibility of similar disclosures (in a privacy notice), unless legal exemptions apply. These disclosures may include:

1. Disclosures made in accordance with a legal obligation, such as a court order or statutory duty;
2. Disclosures made in order to enforce or apply any contract with the data subject; or
3. Disclosures made to protect our rights, property, or safety of our employees, volunteers, contractors or others. This includes exchanging information for the purposes of the prevention or detection of crime

13.2 We will keep records of all information supplied in response to a request for disclosure by a third party and will carefully document any exemptions which may have been applied (including the reasons for their application). Legal advice may need to be obtained in appropriate cases.

13.3 We will abide by the ICO's statutory Data Sharing Code of Practice (or any replacement code of practice) when sharing personal data with other data controllers.

14. SECURITY OF PERSONAL DATA

14.1 Personal data will be processed in a manner that ensures that it is kept appropriately protected and secure, including from unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical and organisational measures.

14.2 We will implement appropriate technical and security measures which ensure a level of security of processing which is appropriate to the risk of processing.

In assessing the appropriateness of technical and organisational measures we shall take into account:

1. the state of the art;
2. the costs of implementation;
3. the nature, scope, context and purpose of processing;
4. the risk (of varying likelihood and severity) for the rights and freedoms of natural persons. In assessing the appropriateness of the level of security we shall, among other relevant considerations, take into account the risks that are presented by the processing involved, in particular the risks which could result from a personal data breach

14.3 We will put in place policies, measures, procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. These may include:

1. Pseudonymisation and encryption of personal data
2. Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. Measures to ensure that we are able to restore availability and access to personal data in a timely manner if there is a physical or technical incident;
4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing.

14.4 The security measure we put in place include:

1. Physical Security
2. Systems Security
3. Organisational Security

15. TRANSFERRING PERSONAL DATA OUTSIDE THE EUROPEAN UNION (EU)

15.1 BMS will only transfer personal data we hold to a country outside the EU if this is permitted under the GDPR. This includes situations where we upload personal data to a cloud the servers of which are situated outside the EU.

15.2 Under the GDPR, we are permitted to transfer data outside the EU in certain circumstances. These include situations where we transfer data:

1. To a country or international organisation which the European Commission declares, by means of a decision, to be a country or international organisation which provides an adequate level of protection (provided that the relevant decision remains in force);

2. Pursuant to a contract which incorporates model contractual clauses which are issued by the European Commission or the ICO in accordance with the GDPR;
3. Pursuant to contractual clauses which are authorised by the ICO;
4. The data subject explicitly consents to the transfer, which consent shall be of the level required in section 5 of this policy and the GDPR;
5. The transfer is necessary for one of the reasons set out in Article 59 of the GDPR, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject

15.3 Satisfying one of the conditions in section 15 does not eliminate the need to comply with all other requirements for processing personal data.

15.4 When we use the services of a cloud service provider (or any other data processor) which requires data to be processed outside the EU we will ensure that we satisfy one of the conditions contained in this section 15 of this policy (or alternatives provided under the GDPR) as well as comply with the requirements relating to the appointment of data processors described in section 20 of this policy.

16. DEALING WITH DATA PROTECTION BREACHES

16.1 All suspected breaches should be reported to the Data Protection Officer.

16.2 We will keep records of personal data breaches, even if we do not report them to the ICO, and such records will be such as to enable the ICO to verity our compliance with the GDPR. The records will be kept by the Data Protection Officer and will describe, as a minimum:

1. The facts relating to the personal data breach;
2. Its effects; and
3. Remedial action taken.

16.3 We are required to report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made within 72 hours from when we become aware of the breach and the time limit starts to run from when any member of staff or contractor becomes aware of the breach and not when reported to dataprotection@bmsworldmission.org.

16.4 When a data protection breach occurs, the Data Protection Officer shall consider the following:

1. Does this policy require amending?
2. Should further guidance be issued about this policy?
3. Do any members of staff require additional training or guidance?
4. Is it appropriate to take disciplinary action?

16,5 A data breach register will be maintained and reported to the Board of Trustees.

17. RECORD KEEPING

17.1 The GDPR requires that organisations not only comply with the law but are able to show that they comply with the law.

17.2 The GDPR specifically requires that we keep, as a minimum, the following records about our processing activities:

1. The name and contact details of any joint controller, any representative and/or Data Protection Officer;
2. The purpose of the processing;
3. A description of the categories of data subjects;
4. A description of the categories of personal data;
5. The categories of recipients to whom the personal data have been or will be disclosed;
6. Transfers to countries or organisations outside the EU (including their identification) and any relevant safeguards;
7. The envisaged time limits for erasure of the different data;
8. A description of security measures taken
9. Reasons for decisions taken

17.3 The GDPR also requires data processors to keep records and when appointing a data processor, we shall require them, in the contract by which they are appointed, to keep such records and to give us access to such records when we require it.

18. DATA PROTECTION BY DESIGN AND BY DEFAULT

18.1 We will implement appropriate technical and organisational measures to ensure that all personal data is processed in accordance with the GDPR, primarily the principles of data protection described in this policy. This includes having safeguards built into our systems which provide for compliance by default.

19. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

19.1 Before carrying out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles and data transfers outside the EU. We may also conduct a DPIA in other cases when we consider it appropriate to do so. Any decision not to conduct a DPIA shall be recorded.

20. APPOINTING DATA PROCESSORS

20.1 When appointing a contractor who will process personal data on our behalf (a data processor) we will, before appointing them, carry out a due diligence exercise to ensure that the relevant processor will implement appropriate technical and organisational measures to ensure that the data processing will meet the

requirements of data protection law, including keeping the data secure, and will ensure protection of the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do so.

21. APPLICATION

21.1 BMS has written procedures designed to ensure this policy is implemented appropriately.

21.2 Our contracted data processors are required to comply with this policy under contract. Any breach of the policy will be taken seriously and could lead to contract enforcement action or termination of the contract. Data processors have direct obligations under the GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

21.3 For data subjects, (see definition at Appendix 1) we will use your personal information in accordance with this policy.

22. POLICY REVIEW

22.1 This policy has been approved by the Board of Trustees which is responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules which apply whenever we obtain, store or use personal data.

22.2 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to dataprotection@bmsworldmission.org.

The Trustees will directly or through delegated authority:

1. Keep the content and effectiveness of this policy under review;
2. Oversee compliance with the policy;
3. Keep a record of all data security incidents or breaches and investigate in appropriate detail;
4. Provide or arrange training and guidance for staff;

The Company Secretary will act as our nominated contact with the ICO.

References in this policy to the Data Protection Officer shall be construed as references to the Data Protection Officer or such other person as the Data Protection Officer may appoint to act on his or her behalf.

22.3 From time to time we may need to make changes to this policy or guidance in line with current operational practices and/or legislation.

22.4 Any questions, ideas or concerns about the operation of this policy or recommendations for additions or amendments should be referred to dataprotection@bmsworldmission.org.

We reserve the right to change this policy at any time. Any amended versions of this policy will take effect from the time they are uploaded to our website. Where appropriate, we will notify data subjects of those changes by mail or by email.

Approved: September 2018

Review date: September 2021

SCHEDULE 1 – RIGHTS OF DATA SUBJECTS

Under the GDPR data subjects have various rights. These are described below. Please note that the descriptions below are only intended to be used as guidance and do not, in any way, affect how they apply under the GDPR. We will apply the rights in accordance with the GDPR which overrides the text of this schedule. Those who wish to obtain more information about this procedure or their data protection rights generally may contact dataprotection@bmsworldmission.org

1. Right of Access

Data subjects have a right to access personal data about them which we hold. It is not a right to documents, but only to personal data contained in documents. This does not cover personal data which relates to other persons. Under the GDPR, requests must be complied with without undue delay and, in any event, within one month of the request. This time limit can be extended to two months where necessary, taking into account the complexity and number of requests. For an extension to apply the data subject must be informed of the extension and why it is needed within one month of the request. If the request is made electronically, the information should be provided in a commonly used electronic form. If more than one copy of the data is requested, we may charge a reasonable fee based on our administrative costs for providing the extra copies. If a request is manifestly unfounded or excessive, we are entitled to refuse to comply with the request or to charge a reasonable fee (based on administrative costs) to deal with the request. We must inform the data subject about this and explain to the data subject that they have a right to complain to the ICO. We will not apply this exception unless we have a strong justification to do so.

2. Right to Rectification

Data subjects may request that we rectify any inaccurate information concerning them and we will comply with such requests as soon as practicable. Data subjects also have a right to have incomplete personal data concerning them completed.

3. Right to Erasure (to be forgotten)

Data subjects are entitled to have their personal data deleted if:

(i) it is no longer needed;
(ii) the only legal ground for processing is consent and the data subject withdraws consent;
(iii) the data subject objects to processing (see the Right to Object below) and there are no overriding legitimate grounds to continue with the processing;
(iv) the data has been processed unlawfully;
(v) the data has to be erased for compliance with a legal obligation which applies to us. There are exceptions to this right. These include when processing is

required for compliance with the law, reasons of public interest, research or statistics, and legal claims.

4. Right to Restrict Processing

Data subjects can in some circumstances demand that processing of their personal data is restricted for a limited time period. The personal data would continue to be held on record, but it cannot otherwise be processed without the data subject's consent. The limited circumstances and time periods are:

(i) if the accuracy of the data is contested, for a period which enables us to verify the accuracy of the data;
(ii) if the processing is unlawful and the data subject opposes the erasure of the data but requests restriction of its use instead;
(iii) if we no longer require the data but the data subject needs the data for the establishment, exercise or defence of legal claims;
(iv) the data subject has objected to data processing (see the Right to Object below), until an assessment is made of whether there are overriding legitimate grounds which can justify the continuation of the processing. Even if the data subject exercises this right we are entitled to process the data in question for purposes relating to legal claims, for the protection of the rights of other persons or for reasons of public interest. We must inform the data subject when the restriction will be lifted.
(v) Right to Object

Where data is processed for the performance of a task carried out in the public interest or legitimate interests pursued by us or a third party, data subjects may object to the processing on grounds relating to their particular situation. In such a case, we will stop processing that data unless there are compelling legitimate grounds for the processing to continue or if the processing is required in connection with legal claims. Data subjects can object to the processing of their data for purposes of direct marketing. This is an absolute right and the processing should cease on request. When data is processed for research or statistical purposes, data subjects can object on grounds relating to their particular circumstances, unless the processing is required for reasons of public interest.

(vi) Right of Data Portability

Data subjects have a right to receive personal data which they provide to us in a structured, commonly-used, and machine-readable (digital) format and are entitled to transmit that data to any other person if the processing of that data is carried out by automated means and is based on

1. the data subject's consent or

2. is processed out of necessity for the purpose of performing a contract with the data subject. Data subjects may also request that we transfer their data directly to a third party.

This right only applies to personal data which data subjects provided to us in a structured digital format.

(vii) Other Rights

Other rights of data subjects in relation to their personal data which arise under the GDPR consist of the right:

(vi) To be provided with privacy notices;
(vii) To request information about persons to whom their personal data has been disclosed;
(viii) To withdraw consent to processing which is based on consent. Withdrawing consent should be as easy as it is to give consent. Withdrawal of consent does not affect the lawfulness of processing already carried out;
(ix) To make a complaint to the Information Commissioner's Office (https://ico.org.uk/);
(x) Not to be subject to decisions based solely on automated data processing which significantly affect them or which produce legal effects concerning them.

8. Exercising rights

Data subjects who wish to exercise any of the above rights or who have any questions about them should contact our Data Protection Officer by email dataprotection@bmsworldmission.org

Any information provided to data subjects should be provided in a concise, transparent, intelligible and clearly accessible form, using clear and plain language. We are required to provide information on action taken subsequent to a request by a data subject based on the above rights, without undue delay and within one month from when we receive the request. This can be extended by two further months where necessary, depending on the complexity and number of requests. If an extension is required we must inform the data subject within one month of receiving the request and give reasons for the delay. We may refuse to comply with requests that are manifestly unfounded or excessive or, alternatively, we may charge a reasonable charge based on our administrative costs. If no action is to be taken, the data subject must be informed of that fact and the reasons within one month from the date of the request. The data subject must also be informed of their right to make a complaint to the ICO. If a request is made by electronic means, all information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Effective as at 25 May 2018

DEFINITIONS OF DATA PROTECTION TERMS

The GDPR (and this policy) "applies to

(i) the processing of personal data wholly or partly by automated means and

(ii) to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

The first part covers all data processing which involves the use of a computer ('processing' broadly covers all forms of handling of data, including storing and accessing it. The term is defined in more detail below).

The second part covers processing which does not involve a computer, of data which either forms part of a filing system, regardless of how well-structured it is, or which is collected in order to be added to a filing system at a later time (e.g. notes of a telephone conversation which are intended to be transferred to a file), even if the data is not actually added.

The following terms are used throughout this policy and bear their legal meaning as set out within the GDPR. The GDPR definitions are further explained below for the sake of clarity:

Data subjects include all living individuals about whom we hold or otherwise process personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects for whom we are likely to hold personal data include:

(i) Our employees

(ii) Our mission personnel

(iii) Volunteers

(iv) Individuals in key roles in churches in membership, or linked, with us

(v); Trustees

(vi) Supporters

(i) Enquirers
(ii) Residential guests
(iii) Complainants
(iv) Consultants/individuals who are our contractors or employees working for them
(v) Advisers and representatives of other organisations.

Personal data means any information relating to a natural person who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons. In addition, personal data is limited to information about living individuals and does not cover deceased persons.

An 'identified' natural person is one who is identified from the data. An 'identifiable natural person' on the other hand is one who is not identified from the data itself but who can be identified, directly or indirectly, by reference to other data, such as an identification number, location data, an online identifier or to one or more factors specific to that person.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if such decisions are taken alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process and this policy is intended to explain how we will comply with the GDPR.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that, as mentioned above, staff of data processors may also be data subjects).

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Sensitive personal data (referred to as 'special categories of data' in the GDPR) includes information about a person's:

(i) Racial or ethnic origin;

(ii) Political opinions;

(iii) Religious or similar (e.g. philosophical) beliefs;

(iv) Trade union membership;

(v) Health (including physical and mental health, and the provision of health care services);

(vi) Genetic data;

(vii) Biometric data;

(viii) Sexual life and sexual orientation.

Other than in the circumstances described in sections 6.8 and 6.9 below, information relating to criminal convictions and offences should not be processed unless the processing

is authorised by law or is carried out under the control of official authority. This includes information about

(i) allegations of criminal offences;
(ii) proceedings in relation to criminal offences or alleged offences; and
(iii) the disposal of criminal proceedings including sentencing. Sensitive personal data can only be processed under strict conditions, including the data subject's explicit consent (although other alternative conditions can apply in limited, very specific circumstances as described below).