CONTAGIOUS BIBLE MINISTRIES

DATA PROTECTION POLICY 2018

"Data Protection Legislation" means the Data Protection Act 1998, the Privacy and Electronic Communications Regulations (EC Directive) Regulations 2003 (SI 2426/2003 as amended), and all applicable laws and regulations, including any replacement UK or EU data protection legislation relating to the Processing of Personal Data, including, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office.

The Data Protection Legislation ("the Legislation") is concerned with the protection of human rights in relation to personal data. The aim of the Legislation is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected.

During the course of the activities of Contagious Bible Ministries, the Contagious Trustees ("we") will collect, store and process personal data about delegates who attend our conferences and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in Contagious Bible Ministries. This policy sets out the basis on which we will process any personal data we collect from data subjects or that is provided to us by data subjects or other sources.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Legislation and with this policy. The post is held by Lisa Wheatley.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

Processing Personal Data

All personal data should be processed in accordance with the Legislation and this policy. Any breach of this policy may result in disciplinary action.

Processing includes obtaining, holding, maintaining, storing, erasing, blocking and destroying data.

Personal data is data relating to a living individual. It includes employee data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations may be covered. 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.

Examples of personal data are employee details, including employment records, names and addresses and other information relating to individuals, including any third-party data and any recorded information including any recorded telephone conversations, emails or digital images.

Employees and others who process data on behalf of Contagious Bible Ministries should assume that whatever they do with personal data will be considered to constitute processing. Individuals should only process data:

- If they have consent to do so; or
- If they have a legitimate interest to hold and process the data in relation to the operation of Contagious.
- If it is necessary to fulfil the contractual obligation entered into when booking on to a Contagious conference
- or as part of the employer/employee relationship; for example, processing the payroll

- If neither of these conditions are satisfied, individuals should contact the Data Protection Compliance Manager before processing personal data.

Compliance with the Legislation

Employees and others who process data on our behalf have a responsibility for processing personal data in accordance with the Legislation. Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

- be obtained and used fairly and lawfully
- be obtained for specified lawful purposes and used only for those purposes
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for any longer than required for those purposes
- be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected)
- be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction
- not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.

Monitoring the use of personal data

We are committed to ensuring that this Data Protection Policy is put into practice and that appropriate working practices are being followed. To this end the following steps will be taken:

- The Operations Team who deal with personal data are expected to be aware of data protection issues and to work towards continuous improvement of the proper processing of personal data;
- The Operations Team who handle personal data on a regular basis or who process sensitive or other confidential personal data will be more closely monitored;
- All Team members must evaluate whether the personal data they hold is being processed in accordance with this policy. Particular regard should be had to ensure inaccurate, excessive or out of date data is disposed of in accordance with this policy;
- The Data Protection Compliance Manager will update the Trustees annually on compliance with data protection practices and any data breaches. Data breaches will be recorded and investigated to see what improvements can be made to prevent recurrences.

Handling personal data and data security

We will take appropriate technical and organisational steps to guard against unauthorised or unlawful processing.

Manual records relating to delegates will be kept secure. Access to such records will be restricted. Computer files will be password protected. We will ensure that staff and leaders who handle personal data are adequately trained and monitored.

We will ensure that passwords and physical security measures are in place to guard against unauthorised disclosure.

We will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).

Security policies and procedures will be regularly monitored and reviewed to ensure data is being kept secure.

Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files. Particular care will be taken over the destruction of manual sensitive data (written records) including shredding or disposing via specialist contractors.

All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed. Any agent employed to process data on our behalf will be bound to comply with this data protection policy by a written contract. Personal data stored on a laptop should be password protected.

The rights of individuals

The Legislation gives individuals certain rights to know what data is held about them and what it is used for. In principle everyone has the right to see copies of all personal data held about them. There is also a right to have any inaccuracies in data corrected or erased. Data subjects also have the right to prevent the processing of their data for direct marketing purposes.

Any request for access to data under the Legislation should be made to Nick Jackman in writing. In accordance with the Legislation we will ensure that written requests for access to personal data are complied with within 30 days of receipt of a valid request.

When a written data subject access request is received the data subject will be given a description of a) the personal data, b) the purposes for which it is being processed, c) those people and organisations to whom the data may be disclosed, d) be provided with a copy of the information in an intelligible form.

Sensitive data

We will strive to ensure that sensitive data is accurately identified on collection so that proper safeguards can be put in place. Sensitive data means data consisting of information relating to an individual's

- Personal information of children under 16 (including name, D.O.B, address, mobile phone number, email address, social media profiles)
- Racial or ethnic origin
- Religious beliefs
- Physical or mental health
- Sexual life
- Criminal offences

Sickness records are likely to include sensitive data and as such should only be held if the explicit consent of each employee is obtained or if one of the other conditions for processing sensitive data is satisfied.

Changes to this policy

We reserve the right to change this policy at any time. Where appropriate we will notify data subjects of those changes by mail or email.

Policy adopted on ……..

Reviewed on……

INFORMATION SECURITY POLICY 2018

Information security involves maintaining the integrity of Contagious data, preventing unauthorised access and disclosure, and safely facilitating access to information when required by authorised users.

'Contagious data' means any personal data of our staff, leaders, customers, delegates or suppliers that is collected, held, processed or shared by or on behalf of Contagious Bible Ministries (CBM).

Information security is the responsibility of every trustee, member of staff, leader, volunteer and supplier using Contagious data on, but not limited to, Contagious information systems.

This policy is the responsibility of the Operations Team who will undertake supervision of the policy. Our IT systems may only be used for authorised purposes. Any person using the IT systems for unauthorised purposes may be subject to disciplinary and/or legal proceedings.

We will ensure information security by:

- Developing and maintaining online data storage methods that comply with EU Data Protection standards.
- Contagious Data will only be shared with people with legitimate interest for the charitable purposes of CBM.
- Any information that has to be transported will be done so safely.
- Implementing controls and checks to prevent data being accidently lost or exposed.
- Contagious data that is required to be retained will be securely archived in online digital storage facilities and password protected.
- Regularly review data stored and permanently delete all records outside of the retention period unless a Data Protection Audit Form has been completed and approved by the Data Protection Compliance Manager.
- Regularly review Contagious data stored on our suppliers' platforms to ensure that all records held outside of the retention period are permanently deleted.
- Contagious data held by the Operations Team will be stored on equipment that is encrypted and pass word protected.
- Any personal equipment which has been used to store or process Contagious data will be disposed of securely when no longer being used.

All breaches of this policy must be reported to Lisa Wheatley at lisa.wheatley@contagious.org.uk

This policy will be regularly reviewed and audited.

Policy adopted on ……..

Reviewed on……

CONTAGIOUS BIBLE MINISTRIES

RETENTION OF RECORDS POLICY 2018

Storage of Data and Records Statement

1. All data and records will be stored in accordance with the security requirements of the Data Protection Legislation and in the most convenient and appropriate location having regard to the period of retention required and the frequency with which access will be made to the record.

2. Data and records which are active will be stored in the most appropriate place, including staff and volunteers' devices, online shared cloud storage systems, email account providers, online booking systems, systems used by our venues, online Customer Relationship Management (CRM) systems and accounting packages for the purposes of Contagious Bible Ministries, commensurate with security requirements.

3. Data and records which are no longer active, due to their age or subject, will be stored in the most appropriate place, including online shared cloud storage systems, email account providers, online booking systems, online CRM systems and accounting packages for their purpose.

4. The degree of security required for file storage will reflect the sensitivity and confidential nature of any material recorded. The table below 'Guidelines for Safe Storage and Sharing of Personal Data' acts as a guide to show how data will be stored and shared.

5. Data and records should not be kept for longer than is necessary (see Guidelines for Retention of Personal Data table below). 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". Some personal data will be held for longer if there is a legitimate interest for retaining the information (e.g. safeguarding records) in compliance with other statutory regulations or recommended good practice. The Operations Team will advise all staff, volunteer leaders and venues to delete or destroy all shared personal data that would no longer be deemed 'current'.

6. Any data that is to be disposed will be safely disposed of for example by shredding or permanently deleted from devices and back-up systems.

Guidelines for Safe Storage and Sharing of Personal Data

DATA SENSITIVITY	SECURITY OF FILE STORAGE
Church contacts, subscribed CRM past contacts, past Dietary/SEN/Medical data, and all legitimate interest data.	Password protected devices/storage systems, Operations Team only, encrypted devices. Any person outside of the Operations Team will complete a Data Audit Form and obtain approval from Lisa Wheatley to store data on other devices (e.g. prayer lists).
Current Leaders data	Files shared with team to be Password protected.
Current Delegates data	Files shared with Senior Team as required to be password protected.
Current Delegates Dietary, SEN, Medical data	Files shared with appropriate team or venues as required and to be password protected
Safeguarding concerns	Data only online in secure password protected cloud storage (paper records to be scanned, securely stored online and hard copies

	destroyed) and shared strictly to persons on a need to know basis with the approval of the Safeguarding Lead or Safeguarding Trustee.
Safeguarding Records	Data only online in secure password protected cloud storage (paper records will be scanned, securely stored online and hard copies destroyed). Sharing of records strictly to persons on a need to know basis with the approval of the Safeguarding Lead or Safeguarding Trustee.
Medical Records	Data only online in secure password protected cloud storage (paper records will be scanned, securely stored online and hard copies destroyed). Sharing of records strictly to persons on a need to know basis with the approval of the Safeguarding Lead.
Delegate Personal Card or bank details	No payment card details are retained by CBM or our online providers. Bank details of staff, some volunteers, delegates/parents of delegates and other organisations are securely held on password protected and encrypted devices by our Operations Team.

Guidelines for Retention of Personal Data

If you have any queries regarding retaining or disposing of data please contact **Lisa Wheatley at lisa.wheatley@contagious.org.uk**

TYPES OF DATA	DATA RETENTION PERIOD
Church Contacts, contact details of enquirers with a legitimate interest who have not subscribed to an update service.	• Period of 13 months after last conference attended/enquiry made, to allow time to invite person to subscribe to update list.
Information about adult parents of delegates who attended a conference with a legitimate interest who have not subscribed to our CRM update service	• Period of 13 months after last conference attended/enquiry made, to allow time to invite them to subscribe to update list and inform them of the next event.
Information held on CRM system for which consent was given.	• Personal data held until an individual unsubscribes from the CRM list • When a person unsubscribes, data will be securely destroyed from the CRM list and other records held (unless held for legitimate interest e.g. safeguarding)
Information relating to children or young adult delegates who have attended CBM events.	• Records held showing attendance and any safeguarding information will be held permanently • Dietary, SEN, medical information shared with venues or Team will be destroyed within 3 months after an event. CBM to hold dietary, SEN, medical information for 10 years after the end of the conference attended. • Child or young adult delegate personal information shared with the Team will be destroyed within 3 months after the end of the conference (unless approved for an extended period for a legitimate reason by the Data Manager) • Child or young adult delegate personal information stored by CBM Operations Team will be securely held for 13 months after an event and considered legitimate interest for cross referencing

	with current bookings to provide safe and quality care for the delegates. • 13 months after a CBM event, other personal data from that event, will be securely destroyed (except safeguarding records that are securely held permanently).
Personal information of suppliers, venues and contacts within other organisations,	• The Operations team will hold personal information of contacts in other organisations for a period of three years after the date of the last communication for the ongoing legitimate purposes of CBM.
Conference Accident Books, Risk Assessment records, Completed Incident Forms, Medication Administration Records and other health & safety records	• 10 years after the date of the last entry.
Safeguarding incident forms, Safeguarding communication records, attendance registers and other sensitive documents relating to safeguarding concerns	• Permanent safe and secure online storage for a lifetime.

CBM EMPLOYER RECORDS	
Health records	• 6 months from date of leaving employment • (Management of Health and Safety at Work Regulations)
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
Statutory Maternity Pay records and calculations	• As Above • (Statutory Maternity Pay (General) Regulations 1986)
Statutory Sick Pay records and calculations	• As Above • Statutory Sick Pay (General) Regulations 1982
Application forms/interview notes	• Maximum of one year from the date of the interviews for those not subsequently employed. If employed, retain in personnel file.
Personnel files and notes of disciplinary and grievance hearings.	• 6 years from the end of employment.
Health records where reason for termination of employment is connected with health, including stress related illness	• 3 years from date of leaving employment • (Limitation period for personal injury claims)
Accident Books and Medication Administration Documents	• for Adults: 3 years after the date of the last entry

Policy adopted on ……..

Reviewed on……