The Faith Mission

DATA PROTECTION PRIVACY NOTICE

PUBLISHED MAY 2018

The Faith Mission would be unable to fulfil its ministry without the valuable help we receive through the prayers, gifts and time of our faithful supporters; we appreciate your fellowship and thank God for you all.

We respect the personal information you share with us, will do all we can to keep it safe and are committed to protecting your privacy. We do not share your details with third parties without your consent.

We endeavour to communicate with you respectfully and efficiently. To help us send you only the information about our work which you have explicitly stated you are happy to receive from us our forms give clear choices. This enables us to send the information in ways that are most convenient to you (email, SMS, phone, post) and we include information on how to change your communication preferences whenever we contact you.

If you don't want to hear from us, please let us know by calling 0131 664 5814 or emailing *hq@faithmission.org*

How we collect information about you

We collect information in the following ways:

When you give it to us DIRECTLY including:

- When you contact The Faith Mission (including the Bible College or the Bookshops) to make a donation, register to receive news about our work, sign up to The Faith Mission's online content or you telephone, email, write to or text The Faith Mission, engage with The Faith Mission via social media channels, enrol for one of our events or courses, make purchases from our bookshops or order products from us online.
- When you attend a meeting or an event, fill out a questionnaire or in conversation request more information and provide us with your contact details.

When you give it to us INDIRECTLY

For example, your information may be shared with us via organisations such as Charity Aid Foundation and Stewardship Trust when you give a gift. These organisations will only do so with your consent. You should check their privacy policy when providing your information to understand fully how they will process your data.

When other organisations have permission to share or it is available PUBLICLY

In addition to the details you give us, we may seek further information about you that is publicly available from external sources. We use this to ensure we are contacting you in the most appropriate ways and with the most relevant information.

When we collect information as you use our website

Like most websites, we use 'cookies' to help us make our sites, and the way you use them, better. Cookies are small text tiles that sites transfer to your device (computer, phone or tablet) and make interacting with a website faster and easier – for example, by automatically filling in your name and address in text fields.

The Faith Mission may store information about you and your activity in cookies.

What personal information we might collect from you

If you support us – for example, make a donation, sign up to receive news of our work, volunteer, take part in an event, or order our materials – we will usually collect the following kinds of information, however this list is not intended to be exhaustive:

- Your name
- Your contact details, which may include postal address, email, telephone numbers, along with your preferences as to which of these we should use to contact you in the future
- Your date of birth if this is relevant to your booking or enquiry with us
- Your gender if this is relevant to your enquiry or booking with us, i.e. for accommodation needs etc.
- Bank account details if you make a regular donation by direct debit or standing order
- Debit or credit card details used to donate to us or when ordering resources – this could be online, over the phone or by mail. We will process your information securely and in accordance with the Payment Card Industry Data Security Standards. Your details are only used to complete the transaction requested; we do not store your debit or credit card details. If you have provided them physically, they are securely destroyed once your donation or payment has completed
- Your Gift Aid status

How do we use this information?

The information we gather helps us to send you what you want when you want it; to send you information about our work, to fulfil orders for materials or to book you into one of our events.

We will use your personal information to: provide you with the information, materials or services you have requested; keep you up to date with the work you are supporting; administer your donation, including processing Gift Aid when appropriate; thank you and send a receipt for your gift or donation; ensure we know how you prefer to be contacted; keep a record of your correspondence, donations history, questions you have asked us, or comments or complaints you have made; contact you in your capacity as a representative of a prayer support group, church, school or other organisation.

We collect relevant data about children and young people from the registration or booking forms completed by their parents or guardians in order to ensure their comfort and safety when attending our clubs, camps or young people's events.

We do not sell or share personal details to third parties for the purposes of their marketing.

Legal bases for processing your data:

Consent

From May 2018, we will process supporters' details based on the consent you have given us. New and existing supporters will be asked to complete an appropriate consent form.

Those who have subscribed to receive First magazine and those who have booked for conventions, camps and other events or those who have enrolled on Bible College, Satellite or correspondences courses have given explicit consent for their data to be used for that purpose by completing the application or enrolment form.

We will use the personal information you provide to help us keep you informed of our activities, meetings or events.

Legitimate Interest

We may occasionally process your personal details on the grounds of having a legitimate interest to do so. For example, long standing prayer partners form an essential undergirding of our work; we believe it is in our legitimate interest to keep you informed of the latest prayer needs.

Opting out

You can change or stop what you receive from us by following the instructions at the bottom of any postal communication or email, or you can contact us by phone at any time.

Protecting your personal information

The security of your information is very important to us. We ensure that there are appropriate controls and procedures in place to protect your personal details. For example, information you submit on a physical form will be kept in a secure file. Forms completed online are stored on a secure server. We also use encryption and secure servers when you make a donation via our website.

We review our data protection processes annually, and when need arises, to ensure that your details remain secure.

Your information may occasionally be passed to service providers that perform functions on our behalf, such as sending postal mail and email. These companies may only use your information to perform these functions and may not use it for any other purposes. They are required to destroy this information once the function for which it has been transferred has been carried out.

If required, we may need to disclose your details to the police, regulatory bodies or legal advisors.

Due to servers and cloud-based storage being located worldwide, this may mean that, during the processing of your data, it leaves the European Economic Area (EEA). Although they may not be subject to the same data protection laws as in the UK by submitting your personal information, you are agreeing to this potential transfer, storing or processing at a location outside the EEA.

Keeping your information up to date

We would really appreciate your cooperation by letting us know if your contact or personal details change. This gives us consent to use the updated information and continue to communicate with you.

How long we will keep your information for:

- We will hold your personal information on our systems for as long as is necessary to carry out the activity relevant to your interaction with us
- We will keep a record of any donations you have made for at least seven years
- Legacy gifts are greatly appreciated by The Faith Mission. We may keep information provided by you or your solicitor indefinitely. This allows us to administer the gift and to communicate with the families of those who have made a bequest to us
- Children's and young people's camps and youth weekend booking details will be kept for a minimum of seven years
- If you ask us to cease communications with you, we will do so. However, we may need to keep a record of your details for financial or other reasons

Right of access

You have the right to ask for a copy of the information we hold about you. If there are any discrepancies in the details we provide, please let us know and we will correct them.

If you want to access your information, send a description of the information you want to see and proof of identity by post to Govan House, 548 Gilmerton Road, Edinburgh EH17 7JD. We do not accept these requests by email. This is so we can ensure that we only provide personal information to the right person.

If you have any questions, please contact our headquarters on 0131 664 5814 or email *hq@faithmission.org*. For further information, see the information commissioner's guidance at *www.ico.org.uk*

Changes to this notice

We may change this privacy notice from time to time. If we make any significant changes in the way we treat your personal information, we will make this clear on The Faith Mission, Faith Mission Bible College and Faith Mission Bookshops websites and/or by contacting you directly.

If you have any questions, comments or suggestions about this notice, please contact the Data Protection Officer, The Faith Mission, Govan House, 548 Gilmerton Road, Edinburgh, EH17 7JD or phone 0131 664 5814 or email *hq@faithmission.org*

APPENDIX 2

DATA RETENTION POLICY AND SCHEDULE

FILE DESCRIPTION	STATUTORY PROVISION	RETENTION POLICY	ACTION / END OF RECORD
1. Governance			
Constitution		Permanent	Keep official copy, and paper and digital copy
Statement of faith		Permanent	Keep official copy, and paper and digital copy
Charity registration		Permanent	Keep in OSCR file
Minutes (Official signed copy)		Permanent	Keep in minutes book in fire proof safe
Agendas		Date of meeting + 1 year	Shred
Reports		Date of Meeting + 5 year	Shred
Policy documents		Expiry of policy	General office/archive or shred
Complaints files		Date of resolution of complaint + 6 years	
2. Management			
Correspondence created by chairman, general director, national directors, College principal, Bookshop general and retail Managers, HR manager		Date of correspondence + 3 years	Shred
3. Members (Missionaries)			
Membership register		Permanent	Keep in general office
Members constitution declaration		Period of membership +10 years	Shred
Members death in service cover		Current policy year + 3 years	Shred/delete
Members files		Period of membership + 10 years	Shred
Disclosure vetting	CRB/ DBS/PVG guidelines	Date of check + 6 months or period of membership + 6 months with members consent	Shred
4. Employees			
Interview notes and recruitment records		Date of interview + 6 months	Shred/destroy
Pre-employment vetting, including references and disclosure checks	CRB /DBS/ PVG guidelines	Date of reference/check +6 months	Shred/destroy
Employee personal files		Termination + 7 Years	Shred/destroy
Time sheets, sick pay etc		Current year + 6 Years	Shred/destroy
Annual appraisal/ assessment records		Current year + 5 years	Shred/destroy
Disciplinary proceedings			
• Oral warning		Date of warning + 6 months	Shred/destroy
• 1st written warning		Date of warning + 6 months	Shred/destroy
• 2nd written warning		Date of warning + 12 months	Shred/destroy
• Final warning		Date of warning + 18 months	Shred/destroy

Records relating to injury or accidents at work		Date of incident + 12 years	Review at the end of this period. A further period of retention may be appropriate
Maternity/paternity pay records	Statutory maternity/ paternity regulations	Current year + 3 years	Shred/destroy
Death in service and pension schemes		Current year + 6 years	Destroy
5. Health and Safety			
Accessibility plans	Disability Discrimination Act	Current year + 6 years	Shred/destroy
Accident reporting:	Social Security regulations		
• adults		Current year + 3 years	Shred/destroy
• children		DOB + 25 years	Shred/destroy
COSHH		Current year + 10 years	Review
Incident reports		Current year + 20 years	Shred/destroy
Policy statements		Date of expiry + 1 year	Shred/destroy
Risk assessments		Current year + 3 years	Shred/destroy
Asbestos monitoring		Last action + 40 Years	Shred/destroy
Fire precaution logs		Current year + 6 years	Shred/destroy
6. Administrative			
Employers/public liability insurance certificate		Permanent while the Mission is in existence	Destroy after the dissolution of the Mission
Visitors books		Current year + 2 years	Review to see whether further retention is necessary
7. Finance			
Audited annual accounts	Financial regulations	Current year + at least 7 years	Review
Invoices, receipts, booking forms and other records covered by financial regulations	Financial regulations	Current year + 7 years	Shred/destroy
Debtors records	Limitation Act	Current Year plus 7 Years	Shred/destroy
Petty cash books	Financial regulations	Current year + 7 years	Shred/destroy
8. Property			
Title deeds		Permanent	These should follow the property
Plans		Permanent	Retain whilst operational, follow the property
Maintenance and contractors	Financial regulations	Current year + 6 years	Shred/destroy
Leases		Expiry of lease + 6 years	Shred/destroy
Lettings		Current year + 3 years	Shred/destroy
Maintenance log books		Last entry + 10 years	Shred/destroy
Contractors reports		Current year + 6 years	Shred/destroy

9. Personal Data			
General supporter list	GDPR	Indefinitely (by consent) or until asked to be removed or last contact + 5 years	Shred/Destroy
Prayer and publicity list	GDPR	Indefinitely (by consent) or until asked to be removed or last contact + 5 years	Shred/Destroy
Bible College information list	GDPR	Indefinitely (by consent) or until asked to be removed or last contact + 5 years	Shred/Destroy
Conventions mailing lists	GDPR	Indefinitely or until asked to be removed	Shred/Destroy
First magazine subscription list	GDPR	Current subscription year + 7 years	Shred/Destroy
Children's and youth club, camp and activities booking forms	GDPR and financial regulations	Current year + 7 years	Shred/Destroy
Photo consent forms	GDPR	Current year + 3 year	Shred/Destroy

APPENDIX 3

DATA BREACH POLICY

1. Introduction

The Mission is obliged under data protection legislation to have in place a framework designed to ensure the security of all personal data during its lifecycle. This policy sets out the procedure to be followed in the event of a breach of our data and information security. It relates to all personal and sensitive data held by the Mission regardless of format and applies to all members, employees, volunteers and students.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

2. Breach definitions

For the purpose of this policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of data either accidentally or deliberately.

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or the equipment on which such data is stored; e.g. loss of laptop, tablet, USB stick, or paper record
- system or equipment failure resulting in a compromise of data
- unauthorised use of, access to or modification of data or information systems
- attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- unauthorised disclosure of sensitive/confidential data
- human error
- 'blagging'; offences where information is obtained by deceiving the organisation which holds it

3. Reporting

Any individual who accesses, uses or manages the Mission's information is responsible for reporting to the Data Protection Officer any data breach and information security incidents immediately, or as soon as possible

The report must include full and accurate details of the incident:

- when the breach occurred (dates and times)
- who is reporting it
- if the data relates to people, the nature of the information, and how many individuals are involved.

Breaches of data protection legislation may result in the Mission's disciplinary procedures being instigated.

4. Containment and recovery

The Mission's Data Protection Officer (DPO) or a Lead Investigating Officer (LIO) appointed by them will:

- determine if the breach is still occurring. If so, the appropriate steps to be taken immediately to minimise the effect of the breach
- take steps to assess the severity of the breach
- establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause
- establish who may need to be notified as part of the initial containment and will inform the police, where appropriate

External support may be sought in resolving the incident promptly.

5. Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered/reported. This will include assessing the risks to individuals, how serious those risks are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- what protections are in place, e.g. passwords, encryptions, etc
- what has happened to the data, e.g. has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- whether there are wider consequences to the breach

6. Notification

The DPO in consultation with the LIO will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so will where feasible, notify them within 72 hours of becoming aware of the breach.

Any incident should be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under data protection legislation
- whether notification would assist the individual(s) affected, e.g. could they act on the information to mitigate risks?
- whether notification would help prevent the unauthorised or unlawful use of personal data
- whether there are any legal/contractual notification requirements
- the danger of unnecessarily notifying; not every incident warrants notification and in some cases could cause needless concern and extra work

Where it has been considered likely to result in a high risk of adversely affecting any individual's rights and freedoms those individuals whose personal data has been affected by the incident will be informed without undue delay.

Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and will include what action has already been taken to mitigate the risks.

Individuals will also be provided with a way in which they can contact the Mission for further information on what has occurred.

The DPO and/or LIO must consider notifying third parties such as the police, insurers, banks or credit card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur as a result of the breach.

A record will be kept of any breach of personal data, regardless of whether notification was required.

7. Review

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies or procedures should be undertaken.

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

APPENDIX 4

DATA SECURITY PROCEDURES

Personal data protection

Personal data (any information that can be linked to an individual) will be protected by the following measures.

Physical protection

- office doors will be protected by external quality locks
- office windows will be closed out of office hours (responsibility of office user)
- physical data (documents) will be kept in locked drawers or filing cabinets
- devices storing or accessing data will be protected by a password (computers, mobile phones, tablets, portable storage, etc.) - data on devices that cannot be password protected will be in password protected files
- data will not be stored on computers which are freely open to multiple users
- unattended computers will be logged off or utilise a password protected screen saver
- offices where data is being processed (including documents left on desks and filing trays) will be locked when unattended
- data will only be accessed by authorised personnel who need to see it and not disclosed to others except as required for the operation of the Mission or by law
- data will never be accessed or used for private/personal purposes
- data stored on personal devices for use elsewhere (e.g. at home) will be immediately returned and/or deleted from storage when the task is complete
- electronic data will be backed up at regular intervals or mirrored in cloud storage
- data will not be kept longer than necessary - retention times will be set for different types of data according to legal and organisational requirements
- documents which are no longer required will be shredded
- storage devices (e.g. hard drives) will be low-level formatted before re-assignment or disposal

Local network protection

- networked computers and devices will be protected by a firewall and, for computers, anti-virus software which will be regularly updated
- email and data storage accounts will be protected by a password, which must not be shared
- care will be taken before posting data via email or instant messaging, giving consideration to whether it is appropriate for the recipient to have the information, the security of both the sending and receiving systems, not sending to unnecessary multiple addresses or mailing lists, and avoiding errors in addressing
- sensitive data will not be posted on social networks (where it can be seen by multiple users) or websites
- sharing of documents via cloud storage will only be with authorised individuals who need access to the information in the course of their responsibilities, and only for as long as necessary

IT and PCI infrastructure protection

The following are the key requirements and procedures taken from our payment card and information technology security policy. The policy is in keeping with the Payment Card Industry (PCI) standard requirements. Those processing payments by card machines should familiarize themselves with the full security policy.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use therefore: Employees handling sensitive cardholder data should ensure that they:

- Handle Mission and cardholder information in a manner that fits with their sensitivity
- Limit personal use of Mission information and telecommunication systems and ensure it doesn't interfere with your job performance
- Understand that the Mission reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose
- Do not use email, internet and other Mission resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal
- Do not disclose personnel information unless authorised
- Protect sensitive cardholder information
- Keep passwords and accounts secure
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended
- Information security incidents must be reported, without delay, to a line manager and recorded in the IT Helpdesk at *http://helpdesk.fmbookshops.com*

Acceptable use

The following guidelines regarding acceptable use should be followed:

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes card holder data
- Employees should ensure that technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts
- Authorised users are responsible for the security of their passwords and accounts
- All pcs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature
- All POS (point of sale) and PIN (personal identification number) entry devices should be appropriately protected and secured so they cannot be tampered with or altered
- Because information contained on portable computers is especially vulnerable, special care should be exercised
- Postings by employees from a Mission email address to newsgroups are not permitted unless posting is part of their business duties. In such cases, any posting should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Mission
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code

Access to the sensitive cardholder data

All access to sensitive cardholder information should be controlled and authorised. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder information should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access to sensitive cardholder information such as PANs, personal information and business data is restricted to employees that have a legitimate need to view such information
- No other employees should have access to this confidential data unless they have a genuine business need
- Where cardholder data is shared with a service provider (third party) a list of such service providers will be maintained

- The Mission will ensure a written agreement that includes an acknowledgement is in place that the service provider will be responsible for the cardholder data that the service provider possesses
- The Mission will ensure that there is an established process including proper due diligence is in place before engaging with a service provider
- The Mission will have a process in place to monitor the PCI DSS compliance status of the service provider

Disposal of stored data

- All data must be securely disposed of when no longer required by the Mission, regardless of the media or application type on which it is stored
- An automatic process must exist to permanently delete on-line data, when no longer required
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons

Incident response plan

Employees of The Faith Mission will be expected to report to the security officer for any security related issues.

The Faith Mission PCI security incident response plan is as follows:

1. Each department must report an incident to the information security officer (preferably) or to another member of the PCI response team
2. That member of the team receiving the report will advise the PCI response team of the incident
3. The PCI response team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident
4. The PCI response team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary
5. The PCI response team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution
6. If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the security officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately
7. A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform The Faith Mission PCI incident response team. After being notified of a compromise, the PCI response team, along with other designated staff, will implement the PCI incident response plan to assist and augment departments' response plans

APPENDIX 5

Data Protection Form

Your interest in and support of the work of The Faith Mission is greatly appreciated. However, to keep you up to date with all the news, activities and events, we need your permission to stay in touch.

Please complete and return this form if you wish to receive new and updates about the work of The Faith Mission.

* required

ABOUT YOU

Please note that we respect your privacy and will keep your data secure. You may ask us to tell you what information we hold about you and, at any time, ask us to delete that data.

Your surname * .....

Your first name * .....

Your address including post code * .....

.....

Your preferred phone number .....

Your preferred email address .....

WHY DO WE COLLECT AND USE YOUR INFORMATION?

The Faith Mission collect and use your information to contact you with various updates regarding the work of The Faith Mission and to comply with any legal requirements. We do not share your information with others unless required to by law. The information comes under 3 sections:

1) General Supporter Information List – information held in connection with those who support the work prayerfully or practically, including a Gift Aid register
2) Prayer and Publicity List – for those who receive Prayer Diary and Prayer Focus as information on the wider work of The Faith Mission including, but not limited to College News, conventions, conferences and Bible weekends and camp ministry
3) Bible College Information List – for those who receive College related news only

THE INFORMATION YOU WOULD LIKE TO RECEIVE

If you wish to receive information from us **please tick box one** and **either** box two or three

Please include me on the: 1. General Supporter Information List ☐ **AND**

2. Prayer and Publicity List ☐

3. Bible College Information List ☐

Signature ..... **Date** .....

Please return your completed form to: The Faith Mission, (local address to be added)