RUGBY STREET PASTORS DATA PROTECTION POLICY

TABLE OF CONTENTS

Purpose of the policy

1.1. Rugby Street Pastors (the local initiative) is committed to complying with privacy and data protection laws including:

(a) the General Data Protection Regulation (**GDPR**) and any related legislation applying in the UK, including without limitation, any legislation derived from the Data Protection Act 2018:

(b) the Privacy and Electronic Communications Regulations 2003 and any successor or related legislation, and,

(c) All other applicable laws and regulations related to the processing of personal data and privacy, including, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office (**ICO**), Ascension Trust or any other supervisory authority.

(d) This policy came into force on 25 May 2018.

1.2. This policy sets out what Rugby Street Pastors will do to protect the personal data of individuals.

1.3. Anyone who handles personal data in any way on behalf of Rugby Street Pastors must ensure that they comply with this policy. Section 3 of this policy sets out what comes within the definition of "personal data". Any breach of this policy will be taken seriously and may result in disciplinary action. It may also expose Rugby Street Pastors to regulatory action from the ICO and other supervisory authorities.

1.4. This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

2. About this policy

2.1. The types of personal data that the local initiative may handle includes details of

Members of the public, Street Pastors and Street Pastor personnel such as Coordinators, Prayer Pastors, School or College Pastors, Rail Pastors, Retail Pastors, Response Pastors, employees, volunteers, Street Pastor trustees/management committee members, emergency contacts, supporting local church ministers, job applicants, job applicants and their referees, volunteers, donors, supporters, applicants volunteering to work with the local initiative and/or their referees, and individuals making enquiries to the local initiative about the work that it does. This list is not exhaustive.

2.2. Dawn Thurkettle, Coordinator for Rugby Street Pastors is responsible for ensuring compliance with the GDPR and this policy. Any questions or concerns about this policy should be referred in the first instance to Dawn Thurkettle (with oversight of data protection), and then to Ascension Trust's Legal & Policy Officer who can be contacted at legal@ascensiontrust.org.uk or on 020 8329 9648.

3. Definitions of data protection terms

3.1. The following terms will be used in this policy and are defined below:

3.2. **Data Subject** includes all individuals about whom Rugby Street Pastors hold personal data, for instance a volunteer, an employee or a supporter. A data subject need not be a UK national or a resident. All data subjects have legal rights in relation to their own personal data.

3.3. **Personal Data** means any information relating to a living person who can be identified directly or indirectly from that information (or from that information and other information in the local initiative's possession). Personal data can be factual (e.g. a name, address, date of birth, email address) or it can be an opinion about that person (e.g. a performance appraisal). Personal data can also include an identifier such as an ID number, location data, an online identifier e.g. an IP address, specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4. **Data Controllers** are the people or organisations who decide the purposes and the means for which any personal data is processed. They have responsibility to process personal data in compliance with the legislation. Rugby Street Pastors is the data controller of all personal data that it manages in connection with its work and activities.

3.5. **Data Processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include other organisations such as website hosts, fulfilment houses, payroll companies or other service providers handling personal data on behalf of the local initiative.

3.6. **European Economic Area** (EEA) includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.7. **ICO** means the Information Commissioner's Office, the authority overseeing data protection regulation in the UK and the lead data protection supervisory authority for Street Pastor initiatives in the EU.

3.8. **Processing** is any activity that involves use of personal data, whether or not by automated means. Processing includes but is not limited to:

(a) collecting;

(b) recording;

(c) organising;

(d) structuring;

(e) storing;

(f) adapting or altering;

(g) retrieving;

(h) disclosing by transmission (e.g. emailing);

(i) disseminating or otherwise making available (e.g. by emailing);

(j) alignment or combination;

(k) restricting;

(l) erasing; or

(m) destruction of personal data.

3.9. **Sensitive Personal Data** (which is defined as "special categories of personal data" under the GDPR includes information about a person's:

(a) racial or ethnic origin;

(b) political opinion;

(c) religious, philosophical or similar beliefs;

(d) trade union membership;

(e) physical or mental health or condition;

(f) sexual life or orientation;

(g) genetic data;

(h) biometric data; and

(i) such other categories of personal data as may be designated as special categories of personal data under legislation.

3.10. **Criminal Offence Data** is no longer classed as sensitive personal data under the GDPR. Criminal offence data is personal data relating to criminal convictions and offences, or related proceedings.

4. Data protection principles

4.1. Anyone processing personal data must comply with the six data protection principles set out in the GDPR. Rugby Street Pastors are required to comply with these principles (summarised below), and to document that the local initiative complies, in respect of any personal data that it deals with as a data controller.

4.2. Personal data should be:

(a) processed fairly, lawfully and transparently;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary for the purpose for which it is held;

(d) accurate and, where necessary, kept up to date;

(e) not kept for any longer than is necessary; and

(f) processed in a manner that ensures appropriate security of the personal data.

5. Processing data fairly and lawfully

5.1. The first data protection principle requires that personal data is obtained fairly and lawfully and processed for the purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where is it necessary for the performance of a contract.

5.2. To comply with this principle, where appropriate and when an individual does not already have the information, the local initiative will provide a privacy notice to data subjects The privacy notice will contain the following information:

(a) the type of information the local initiative will be collecting (categories of personal data concerned);

(b) who will be holding the data subject's information, i.e. Rugby Street Pastors, including the local initiative's contact details;

(c) why the local initiative is collecting the data subject's information and what it intends to do with it;

(d) the legal basis for collecting their information;

(e) if the local initiative is relying on legitimate interests as a basis for processing, what those legitimate interests are;

(f) whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;

(g) the period for which their personal data will be held or, where that is not possible, the criteria that will be used to decide that period.

(h) details of people or organisations with whom the local initiative will be sharing their personal data;

(i) if relevant, the fact that the local initiative will be transferring their personal data outside the EEA and details of relevant safeguards; and

(j) the existence of any automated decision-making including profiling in relation to that personal data.

See Schedule 4 for Rugby SPI Privacy Policy

5.3. What are the lawful bases for processing?

At least one of these must apply whenever the local initiative processes personal data:

(a) **Consent**: the individual has given clear consent for the local initiative to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract the local initiative has with the individual, or because the individual has asked the local initiative to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for the local initiative to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for the local initiative to perform a task in the public interest or for the local initiative's official functions, and the task or function has a clear basis in law.

(f) **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

5.4. Where the local initiative obtains data about a person from a source other than the person themselves, it must provide the data subject with the following information in addition to that listed under 5.2 above, where appropriate and where the data subject does not already have this information;

(a) The categories of the personal data that the local initiative holds; and

(b) The source of the personal data and whether this is a public source.

5.5. In addition, in both situations set out in 5.2 and 5.3 above, (where personal data is obtained both directly and indirectly) the local initiative must also inform individuals of their rights outlined in section 9 below (Rights of individuals under the GDPR), including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data.

6. Processing data for the original purpose

6.1. The second data principle requires that personal data is only processed for purposes compatible with the specific, explicit and legitimate purposes that the data subject was told about when the local initiative first obtained their information.

6.2. This means that the local initiative should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a data subject's personal data for a new purpose, the individual may need to be informed of the new purpose beforehand. For example, if the local initiative collects personal data such as a contact number or email address in order to update a person about the local initiative's activities, it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without notifying that person.

7. Personal data should be adequate and accurate

The third and fourth data protection principles require that personal data kept by the local initiative should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out of date personal data must be destroyed securely, and the local initiative must take every reasonable steps to ensure that inaccurate personal data is corrected.

8. Not retaining data longer than necessary

8.1. The fifth data protection principle requires that the local initiative should not keep personal data for longer than it needs for the purpose for which it was obtained. This means that the personal data held by the local initiative should be securely destroyed or deleted from the initiative's systems when it is no longer needed. Anyone believing

that the local initiative is holding out of date or inaccurate personal data should contact Dawn Thurkettle.

8.2. Records of Street Pastor personnel (coordinators, Street Pastor volunteers, Prayer Pastors, management committee members/trustees, etc.) should be retained whilst they are in post, and then for the period set out in the Data Retention Policy in **SCHEDULE 1** of this policy.

8.3. If personal data is archived, please remember that any archived personal data needs to be included in any subject access request.

9. Rights of individuals under the GDPR

9.1. The GDPR gives individuals rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of Rugby Street Pastors needs to be aware of these rights. They include, but are not limited to, the right:

(a) to be told, where any information is collected from the person directly, any available information as to the source of the information (right to be informed);

(b) to request a copy of any personal data that Rugby Street Pastors holds about them (as data controller), as well as a description of the type of information that the local initiative is processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will need to be stored (the right of access). This particular right is known as subject access rights and data subjects have the right to make what is known as a subject access request (SAR). Guidance on responding to a SAR is set out in **SCHEDULE 2** to this policy;

(c) where appropriate, to have inaccurate data amended or destroyed (right to rectification);

(d) where appropriate, to have all their personal data erased (the right to be forgotten/right to erasure) unless certain conditions apply;

(e) where appropriate, to restrict processing where the data subject has objected to the processing (right to restrict processing);

(f) where appropriate, to prevent processing that is likely to cause unwarranted substantial damage of distress to the data subject themselves or anyone else (right to restrict processing);

(g) where appropriate, to obtain and reuse their personal data for their own purposes across different services (right to data portability);

(h) where appropriate, to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests (right to object); and

(i) where appropriate, to be told of the existence of any automated decision-making with their personal data (rights related to automated decision making including profiling).

10. Data security

10.1. The sixth data protection principle requires the local initiative to keep secure any personal data that it holds.

10.2. The local initiative is required to put in place procedures to keep personal data that it holds secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.3. When dealing with sensitive personal data (or special categories of personal data), more rigorous security measures are likely to be needed, for example, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device, it should always be encrypted.

10.4. When deciding what level of security is required, the starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5. The following security procedures and monitoring processes must be followed in relation to all personal data processed by the local initiative:

(a) encryption of personal data; measures to restore availability and access to data in a timely manner in event of physical or technical incident;

(b) files containing personal data on a shared PC should be password protected and locked when they are away from the PC to prevent anyone other than the data controller/processor from gaining access;

(c) a process for regularly testing, assessing and evaluating effectiveness of security measures;

(d) backing up data; data controllers from the local initiative should ensure that individual monitors do not show confidential information to passers-by and that they securely log off from their PCs when they are left unattended. This will be a particular risk where PCs are shared in a home environment;

(e) paper documents should be shredded, memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when no longer required;

(f) personal data must always be transferred in a secure manner. The degree of the security required will depend on the nature of the data - the more sensitive and confidential the data, the more stringent the security measures should be. Other measures to be taken to ensure confidentiality, integrity, availability and resilience of processing system. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential) and the local initiative's personnel must keep data secure when travelling or using it outside of their home or normal place of work.

10.6. Disclosure and Barring Service (DBS) certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

11. Transferring data outside the EEA

The GDPR requires that when organisations transfer personal data outside of the EEA, they take steps to ensure that the data is properly protected.

11.1. Personal data may be transferred to people or organisations in countries with an EU adequacy agreement without the need to take additional steps beyond those the local initiative would take when sharing personal data with any other organisation. in transferring personal data to other countries outside the EEA (which are not on the approved list), it will be necessary to enter into an EC-approved agreement, seek the consent of the data subject, or rely on one of the other exceptions under the GDPR that apply to the transfer of personal data outside the EEA.

11.2. The EU-US Privacy Shield permits transfer of personal information to organisations that are based in the US and have signed up to the agreement.

12. Processing Sensitive Personal Data

12.1. On some occasions the local initiative may collect information about individuals that is defined by the GDPR as special categories of personal data, and special rules will apply to the processing of this type of data. In this policy special categories of personal data are referred to as "sensitive personal data". The categories of sensitive personal data are set out in the definition section 3.9 above .

12.2. Purely financial information is not defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.

12.3. In most cases, in order to process sensitive personal data, the local initiative must demonstrate that the processing meets a substantial public interest or obtain explicit consent from the data subject involved. As with any other type of information the local initiative will also have to be absolutely clear with data subjects about how their information will be used.

13. Notification

13.1. Rugby Street Pastors will consult with the ICO where necessary when carrying out "high risk" processing.

13.2. The local initiative will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary within 72 hours. The local initiative will also notify affected individuals where the breach is likely to result in high risk to the rights and freedoms of these individuals.

14. Monitoring and review of the policy

14.1. This policy will be reviewed annually by the Rugby Street Pastor Board of Trustees/management committee to ensure that it is achieving its objectives.

15. Criminal Offence Data

15.1. Local initiatives will need to have a lawful basis for processing criminal offence data, e.g. DBS checks, in the same way as for any other personal data; however, they will not be able to maintain a register of criminal convictions as they are not an official authority for that purpose. Please refer to **SCHEDULE 3** to this policy for guidance on the on the Handling of DBS Certificate Information.

16. Adoption of policy

This policy was adopted by the Management Committee of Rugby Street Pastors on the date set out below.

First Prepared	June 2018	**Approved**	**Sep 18**
By	Matthew Deaves, Pete Hickey & Bob Reeve	**Signed**	Adopted by RSPI Management Committee 17 Sep 18
Issue Date	18 September 2018	**Issue Version**	V2.0
Last Reviewed	10 June 2019	**Issue Version**	V3.0
Next Review	**June 2020**		

SCHEDULE 1
Street Pastor Data Retention Policy

Type of Personal Data	Retention Period	Additional Retention Period
Recruitment records: Personal data on application forms and associated documents.	If the application is granted and an appointment made, the application form and any associated documents will form part of that individual's personnel records. If the application is rejected the application form and any associated documents should be deleted after a period of 4 months.	If an applicant makes an appeal regarding an unsuccessful application within the initial retention period, then for three months beyond the period taken to resolve the appeal if that period falls outside of the initial retention period.
Volunteer personnel records (Coordinator, Street Pastor, Prayer Pastor, School Pastor)	2 years following cessation of the volunteer's role within the local initiative.	If the volunteer makes a complaint or is subject to a complaint within the initial retention period, then for six months beyond the period taken to resolve the complaint if that period falls outside of the initial retention period. Information about the local initiative's volunteers may be kept for historical and research purposes.
Trustee or management committee member personal records	1 year after they step down from their role.	If the trustee has served their full term of office and indicates that they intend to reapply for the role after a year, then for an additional period of six months to allow them to reapply and their application to be considered.

Type of Personal Data	Retention Period	Additional Retention Period
DBS records	Once a recruitment (or other relevant) decision has been made, the certificate information should not be kept for any longer than is necessary. This is generally for a period of up to 6 months, to allow for the consideration and resolution of any disputes or complaints.	In very exceptional circumstances, it is considered necessary to keep certificate information for longer than 6 months, the local initiative will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so.
Supporter details / Photography & Video	For as long as they have opted in to receiving fundraising communications. Consents should be updated every 2 years. If they opt-out from fundraising communications keep sufficient information to ensure that the local initiative does not inadvertently contact the donor, i.e. a no contact list. All other data to be deleted within 3 months.	Indefinitely on a no contact list where they have opted out of receiving communications.
Supporting church leadership details	For as long as the church continues to support the local initiative, with leadership details updated/deleted as necessary.	

SCHEDULE 2
Street Pastor Guidance on Subject Access Requests

1. Individuals (data subjects) have the right to access their personal data and supplementary information.

2. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

3. A request for access to personal data is known as a subject access request (SAR). A SAR is simply a request made by or on behalf of an individual (the data subject) for the information which he or she is entitled to ask for when exercising their right of access under the GDPR. The request does not have to be in any particular form, nor does it have to include the words "subject access request" or make any reference to the relevant legislation. A request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act.

4. Under the GDPR, individuals normally have the right to obtain:

   - confirmation that their data is being processed;
   - access to their personal data; and
   - other supplementary information - this largely corresponds to the information that should be provided in a privacy notice (see 5.2 above).

5. If requested, the local initiative must normally provide a copy of the information free of charge. However, it can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive. Compliance with a subject access request can in some instances be time consuming and the cost of providing copy documents can be expensive.

6. The local initiative may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that the local initiative can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

7. The local initiative should ensure that it has enough information to be sure of the requester's identity and if necessary, request further information to verify their identity.

8. Information must normally be provided without delay and at the latest within one month of receipt of the SAR, or receipt of any additional information requested from the individual to verify their identity. If the local initiative is to charge for a SAR, then the time limit starts to run from receipt of any payment.

9. The local initiative will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the individual making the request must be informed within one month of the receipt of the request, explaining why the extension is necessary.

10. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the local initiative can:

(a) charge a reasonable fee taking into account the administrative costs of providing the information; or

(b) refuse to respond.

Where the local initiative refuses to respond to a request, an explanation must be given to the individual making the request explaining why, informing them of their right to complain to the ICO and to a judicial remedy. This explanation must be given without undue delay and at the latest within a month.

11. The local initiative must verify the identity of the person making the request, using "reasonable means". For example, the requester may be asked to produce a copy of official ID documents like a current passport or driver's licence.

12. If the request is made electronically, the local initiative may provide the information in a commonly used electronic format, e.g. by email.

13. If the address is made in writing, the local initiative may provide the information by hard copy, unless the data subject agrees to the information being provided in a commonly used electronic format.

14. The right to obtain a copy of the information must not adversely affect the rights and freedoms of others, so where the information to be provided identifies another data subject, that third party's name and any other personal data should normally be redacted.

15. The local initiative does not have to comply with a SAR if to do so would mean disclosing information about another individual who can be identified from that information, except where:

(a) the other individual has consented to the disclosure; or

(b) it is reasonable in all the circumstances to comply with the request without that individual’s consent.

If necessary information can be redacted to conceal that other individual's identity if this is possible.

Confidentiality is one of the factors the local initiative must take into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises where information that is not generally available to the public (ie, genuinely confidential information) has been disclosed to the local initiative with the expectation it will remain confidential. This expectation might result from the relationship between the parties. For example, the following relationships may carry with them a duty of confidence in relation to information disclosed.

- Pastoral (minister and member of their congregation e.g. in the provision of a reference in support of a Street Pastor application)
- Medical (doctor and patient)
- Employment (employer and employee)
- Legal (solicitor and client)

- Financial (bank and customer)
- Caring (counsellor and client)

However, the local initiative should not always assume confidentiality. For example, a duty of confidence does not arise merely because a letter is marked "confidential" (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so does not have the 'necessary quality of confidence'), or there may be other factors, such as the public interest, which mean that an obligation of confidence does not arise.

In most cases where a duty of confidence does exist, it will usually be reasonable to withhold third-party information unless the local initiative has the third-party's consent to disclose it.

16. Where the local initiative processes a large quantity of information about an individual, the GDPR permits the local initiative to ask the individual to specify the information the request relates to, e.g. "Any personal data related to the decision to discipline me and the subsequent disciplinary proceedings."

17. The GDPR does not include an exemption for requests that relate to large amounts of data, but the local initiative may be able to consider whether the request is manifestly unfounded or excessive.

18. For more detailed guidance on responding to subject access requests please read the ICO's Subject Access Code of Practice.

SCHEDULE 3
Street Pastors' Guidance on the Handling of DBS Certificate Information

1. Introduction

This guidance deals with the secure storage, handling, use, retention and disposal of Disclosure and Barring Service (DBS) certificates and certificate information.

2. General principles

2.1. As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, Rugby Street Pastors (the local initiative) complies fully with the Code of Practice regarding the correct handling, use, storage, retention and disposal of DBS certificates and certificate information.

2.2. The local initiative also complies fully with its obligations under the General Data Protection Regulation and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information and has a written policy on these matters, which is available to those who wish to see it on request.

3. Storage and access

Certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties in the recruitment of volunteers or staff members to the local initiative.

4. Handling

4.1. In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. The local initiative maintains a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

4.2. Once the inspection has taken place the certificate should be destroyed in accordance with the Code of Practice.

5. Usage

Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

6. Retention

6.1. Once a recruitment, DBS renewal or other relevant decision has been made, the local initiative will not keep certificate information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints.

6.2. If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, the local initiative will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so.

6.3. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will need to be maintained.

7. Disposal

7.1. Once the retention period has elapsed, the local initiative will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. a waste bin or confidential waste sack).

7.2. The local initiative will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, the local initiative may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

8. Acting as an umbrella body

8.1. Before acting as an umbrella body (an umbrella body being a registered body which countersigns applications and receives certificate information on behalf of other employers or recruiting organisations), the local initiative will take all reasonable steps to satisfy itself that they will handle, use, store, retain and dispose of certificate information in full compliance with the code of practice and in full accordance with this policy.

8.2. The local initiative will also ensure that anybody or individual, at whose request applications for DBS certificates are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

SCHEDULE 4
Rugby Street Pastors Privacy Policy

1. Scope
This privacy notice relates to the Rugby Street Pastors Initiative. It applies to information provided by post, email, text, telephone and online.

2. PRIVACY NOTICE

2.1 The Data Controller
The data controller for Rugby Street Pastors is:

Dawn Thurkettle
Rugby Street Pastors Coordinator
C/O Rugby Elim
46 Cambridge Street
Rugby CV21 3NQ
United Kingdom

We store personal data on local computers with restricted access, and also in the cloud using a data processor, which is Dropbox International Unlimited Company. Dropbox host their servers in the United States and abide by the US EU Privacy Shield.

2.2 Personal data
The personal data we would like to collect from Street Pastors, Prayer Pastors and the Street Pastors management team includes your name, age, address and contact details, training and application records, availability for training and Street Pastor and Prayer Pastor rotas, and related information. We will use this data for the following purposes:

- To process your application to be a Street Pastor, Prayer Pastor or Response Pastor;
- To manage the Street Pastors project;
- To make sure you complete your training to be a Street Pastor;
- To administer training and Street Pastor and Prayer Pastor rotas;
- To keep you informed about the scheme.

The personal data we would like to collect from people our Street Pastors meet could include your name, age, address and contact details, and personal circumstances. We will use this data to provide you with a reassuring presence on the street, to protect your vital interests, or to prevent or detect crime.

2.3 Legal basis
The processing is necessary so that we can run the Street Pastors scheme.

Where we need to process information in order to administer the scheme, data protection law describes this processing as in our legitimate interests.

Where we need to process information in order to protect someone from harm, data protection law describes this processing as in their vital interests.

Where we need to process information in order to prevent or detect crime, data protection law describes this processing as in the public interest.

If you do not provide the information we ask for we may not be able to help you, or you may not be able to be part of the Rugby Street Pastors.
Sometimes we have to collect special categories of personal data. This is normally to protect somebody from harm and is in their vital interests, or it is because you are in regular contact in

connection with the legitimate activity of the Street Pastors, which is a not-for-profit body with a religious aim.

2.4 Consent
We do not need your consent to collect or process your personal information in relation to the Rugby Street Pastors. This is because we are relying on alternative legal bases.

2.5 Disclosure
Rugby Street Pastors may pass on your personal data to third parties for the purposes of detecting or preventing fraud or other crime. These organisations may include Rugby First, Warwickshire County Council, Warwickshire Police, the Department of Work and Pensions, or any other organisation where we are required or permitted by law to share information.

We may pass your personal data to the West Midlands Ambulance Service, Warwickshire Police or Warwickshire Fire and Rescue Service, or any other individual or organisation where it is necessary to protect your vital interests.

We may share personal information about our Street Pastors with the Ascension Trust, which is the governing body behind the Street Pastors project.

We share information about individuals we meet as part of our patrols with our Street Pastors team, for training and monitoring purposes and to provide you with a better service.

2.6 Retention period
Rugby Street Pastors will process personal data about Street Pastors for as long as they are part of the scheme and for up to two years afterwards.

2.7 Your rights as a data subject
You have the right:

- to request a copy of the information that we hold about you;
- to correct data that we hold about you that is inaccurate or incomplete;
- in certain circumstances you can ask for the data we hold about you to be erased from our records;
- where certain conditions apply to have a right to restrict the processing;
- in some circumstances, to have the data we hold about you transferred to another organisation;
- to object to certain types of processing such as direct marketing;
- to complain if we refuse a request you may make using these rights and you are not happy with our reason.

We may refer any request you may make using these rights to another organisation, if they have been involved in processing your personal data.

2.8 Complaints
If you are unhappy about how we are handling your personal data you can complain to the Street Pastors Coordinator. You can also complain to Ascension Trust and/or the Information Commissioner's Office.

The details for each of these contacts are:

The Street Pastors Coordinator	**Information Commissioner's Office**
Rugby Street Pastors	Information Commissioner's Office
C/O Rugby Elim	Wycliffe House

46 Cambridge Street	Water Lane
Rugby CV21 3NQ	Wilmslow SK9 5AF
United Kingdom	United Kingdom
	casework@ico.org.uk Tel: 01625 545745

Ascension Trust's Legal & Policy Officer who can be contacted at: legal@ascensiontrust.org.uk or Tel: 020 8329 9648.