SOUTHAMPTON STREET PASTORS DATA PROTECTION POLICY

TABLE OF CONTENTS

not defined.

Purpose of the policy

1.1. Southampton 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 Bill 2017:

(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 comes into force on 25 May 2018.

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

1.3. Anyone who handles personal data in any way on behalf of Southampton 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 Southampton 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

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 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. Mike Sarson, the Operations Manager at Southampton 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 Richard Pitt (Vice Chair of Trustees) 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 Southampton 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 (eg a name, address, date of birth, email address) or it can be an opinion about that person (eg a performance appraisal). Personal data can also include an identifier such as an ID number, location data, an online identifier eg 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. Southampton 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 (eg emailing);

(i) disseminating or otherwise making available (eg 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 principals

4.1. Anyone processing personal data must comply with the six data protection principles set out in the GDPR. Southampton Street Pastors is 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, each time the local initiative receives personal data about a person directly from that individual (the data subject), which it intends to keep, that individual needs to be provided with "fair processing information" also known as a privacy notice. The privacy notice needs to 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, including the local initiative's contact details and the contact details of the local initiative's Data Protection Officer (if there is one);

(c) why the local initiative is collecting the data subject's information and what it intends to do with it, eg to process donations or send them email updates about the local initiative's activities or to process their application to train as a Street Pastor;

(d) the legal basis for collecting their information (eg the local initiative is relying on their consent, or on its legitimate interests, or on some other legal basis);

(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, eg for as long as an individual remains a Street Pastor and for a specified period after their role ceases (see the Street Pastor Data Retention Policy in

SCHEDULE 1).

(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.

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. (This basis cannot apply to public authorities processing data to perform their official tasks.)

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;

(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.

5.6. This privacy notice information can be provided in a number of places including on web pages, in mailing, or on application forms. The local initiative must ensure that the privacy notice is concise, transparent, intelligible and easily accessible.

6. Processing data for the original purpose

6.1. The second data principle requires that personal data is only processed for 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 will 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 first getting that person's consent.

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 should 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 the Operations Manager

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

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

(a) to be told about the use and collection of their personal data (i.e. the privacy information). This includes the purpose for processing their personal data, retention periods, and who it will be shared with). Where personal data is obtained from other sources, individuals must be provided with privacy information within a reasonable time, and no later than a month (right to be informed);

(b) to request a copy of any personal data that Southampton 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 3 to this policy;

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

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

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

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

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

(h) 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) 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 (daily back-ups should be taken of all data on the system and data should not be stored on local drives or removable media as these will not be backed up); 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 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

11.1. The GDPR requires that when organisations transfer personal data outside of the EEA, they take steps to ensure that the data is properly protected. The local initiative may transfer personal data outside the EEA in the following circumstances: when involved in setting up overseas initiatives, when arranging travel for individuals to go on overseas mission, when personnel from the local initiative represents the local initiative abroad, or volunteers with overseas initiatives.

The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include:

Andorra
Argentina
Canada
Guernsey
Isle of Man
Israel
New Zealand
Switzerland
Faroe Islands
Jersey, and
Uruguay

This list may be updated. A list of those countries providing an adequate data protection regime can be found on the European Commission's website.

11.2. Personal data may be transferred to people or organisations in the countries referred to in 11.1 above 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.

11.3. The EU-US Privacy Shield is the provision that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the ICO or Ascension Trust's Legal & Policy Officer, before transferring personal data to organisations in the US.

11.4. The lead data protection supervisory authority for all Ascension Trust initiatives in the EU including Street Pastor is the ICO and the main establishment for Street Pastor initiatives is Ascension Trust in the UK.

11.5. For more information, please contact Ascension Trust's Legal & Policy Officer or seek further legal advice.

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 technically 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 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.

12.4. It is not always necessary to obtain explicit consent; there are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data. If the local initiative is concerned that it is processing sensitive personal data and is not able to obtain explicit consent for the processing, speak to the local initiative's data protection officer or to Ascension Trust's Legal & Policy Officer.

13. Notification

13.1. Southampton Street Pastors recognises that whilst there is no obligation for the local initiative to make an annual notification to the ICO under the GDPR, the local initiative 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 Southampton 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, eg 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 4** to this policy for guidance on the on the Handling of DBS Certificate Information.

16. Useful Links

16.1. For detailed guidance please refer to the ICO's Guide to the GDPR (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) (140 pages). For guidance on all data protection issues for organisations please go to https://ico.org.uk/for-organisations/

16.2. To contact Ascension Trust for further guidance:

Legal & Policy Officer
Ascension Trust
Alpha House158 Garth Road
Morden
SM4 4TQ

legal@ascensiontrust.org.uk
020 8329 9648

16.3. To contact the ICO:

Information Commissioner's Office
Wycliffe House
Water Lane Wilmslow
Cheshire SK9 5AF

www.ico.org.uk

Or if you are in the Republic of Ireland:

Data Protection Commissioner
Canal House
Station Road
Portarlington
R32 AP23
Co. Laois

www.dataprotection.ie

16.4. To contact the Disclosure and Barring Service

DBS customer services
PO Box 3961
Royal Wootton Bassett
SN4 4HF

customerservices@dbs.gsi.gov.uk
DBS helpline: 03000 200 190

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)	1 year following cessation of the volunteer's role within the local initiative. For Street or School Pastors who have not formally stepped down from their role, for a year after their last patrol, after which they will need to reapply with fresh references before resuming patrols.	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.
Employees records	Pension records should be kept indefinitely. 6 months after the end of employment.	If a complaint is made about them, or they make an application to the Employment Tribunal then for six months beyond the period taken to resolve the complaint if that falls outside of the initial retention period. Information about the local initiative's officers and their careers may be kept for historical and research purposes.

Type of Personal Data	Retention Period	Additional Retention Period
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.
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	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, ie 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 Privacy Notices

NB: The internal privacy notice is for use with volunteers, employees, management committee members/trustees.

The general privacy notice is for use with members of the public and individuals external to the local initiative.

Southampton Street Pastors Privacy Notice (Internal)
How the information we hold on you will be used

1. Personal data is any information about a living individual which allows them to be identified (eg a name, email address, address, image, ID number). Identification can be by the information alone or in conjunction with any other information.

2. Your information/personal data will be held by Southampton Street Pastors (the local initiative). You can contact Southampton Street Pastors as a data controller and for any data protection enquires by post by writing to:

   Data Protection Officer
   Southampton Street Pastors
   [Address]

   By email at Southampton@streetpastors.org.uk and by telephone on [telephone number].

3. Southampton Street Pastors is part of a wider network of Street Pastor initiatives in the UK coming under the umbrella of Ascension Trust, a charity registered in the UK, who all work together to deliver the Street Pastors' mission in communities throughout the UK. We may need to share information that we hold with them so that they can carry out their responsibilities in our community. The Street Pastor network and Ascension Trust are joint data controllers and all responsible to you for how your personal data is processed. This privacy notice is sent to you by Southampton Street Pastors on our own behalf and on behalf of these other data controllers.

4. As data controllers we will comply with our legal obligations towards you to keep any information we hold on you up to date; to store and destroy it securely; not to collect or retain excessive or unnecessary amounts of data; to keep your personal data secure, and protect it from loss, unauthorised access, misuse and disclosure.

5. We will use your personal data for some or all of the following purposes:

   (a) to enable us to deliver the Street Pastor mission to our local community, and to carry out other charitable or voluntary activities for public benefit as provided for in the governing document and statutory framework of the local initiative and its other joint controllers;

   (b) to fundraise and promote our work;

   (c) to send you communications which you may have requested or that may be of interest to you about our operations, events, fundraising activities, campaigns and appeals.

   (d) to manage your role as a volunteer, trustee, management committee member or employee;

   (e) to process a donation that you have made (including Gift Aid information);

   (f) to maintain our records and accounts;

   (g) to keep you notified of changes to the service that we provide, events or personnel within the local initiative;

   (h) to seek your comments or views;

   (i) to process applications for a role;

   (j) to share your contact details with Ascension Trust as necessary for the management of your role within the Street Pastor network or the wider Ascension Trust network;

   (k) for legal, personnel, administrative and management purposes, to enable us to meet our legal obligations, eg to pay employees, monitor performance, pay expenses;

   (l) to process sensitive personal data, eg about health, in order to take decisions about your fitness or ability for your role with the local initiative;

   (m) to process sensitive personal data about racial or ethnic origins in order to monitor compliance with equal opportunity legislation;

   (n) to carry out checks with the Disclosure and Barring Service as necessary for your role;

   (o) in order to comply with legal requirements and obligations to third parties;

6. We may process the following information:

   (a) Names, titles, aliases, photographic images.

   (b) Contact details, eg telephone numbers, addresses and email addresses.

   (c) Where relevant we may process demographic information such as your date of birth, marital status, nationality, family composition, dependants, education/work histories, academic/professional qualifications and employment details.

   (d) Non-financial identifiers such as passport numbers, driving licence numbers, tax payer ID number, tax reference codes, and national insurance number.

(e) Where you make donations or pay for activities or merchandise, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

(f) Financial information such as salary, record of earnings, tax code, tax and benefits contributions, expenses claimed, amounts insured and amounts claimed.

(g) Other operational personal data created, obtained, or otherwise processed in the course of the local initiative carrying out its activities including, but not limited to, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, incident logs, injuries and insurance claims.

(h) Other employee data (not already covered) relating to your role with the local initiative including emergency contact information, gender, date of birth, performance management information, immigration status, citizenship, retirement date, employment references and personal biographies.

(i) The data we process will likely include sensitive personal data because as a Christian organisation our volunteers are in the main Christian, which may be suggestive of your religious beliefs. The local initiative may also process other categories of sensitive personal data revealing racial or ethnic origin, religious or philosophical beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health.

(j) The local initiative may also process criminal records and other judicial records.

7. Whilst we will rely on your consent as a legal basis for this processing, we will also have a legitimate interest for processing your personal data in order to assist you in fulfilling your role with the local initiative including administrative support or if processing is necessary for compliance with a legal obligation. Whilst exercising our legitimate interest we will always take into account your interests, rights and freedoms. As a religious organisation we are also permitted to process information about your religious beliefs to administer your role within the local initiative.

8. Where your personal data is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

9. Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of our tasks or where you first give us your prior consent. It is likely that we will need to share your data with Ascension Trust as the umbrella body for Street Pastors. We may also need to share your contact details with other individuals within the local initiative in order to facilitate your role. We may share your personal data with your local church leader for the purpose of your pastoral care.

10. We may also share your personal data with our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software.

11. It is not envisaged that your personal data will be transferred to any party outside of the UK, but in the event that this needs to be done, your consent will be sought beforehand. Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the EU. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

12. We will retain your personal data for as long as you remain in your role, or any other role with Southampton Street Pastors where the information may be required and for a period of time after any role with the organisation ceases, in line with our Data Retention Policy. Elements of your personal data may be retained beyond this initial retention period by the organisation for historical, statistical or research purposes.

13. We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits. In general, we will endeavour to keep data only for as long as we need it and we will delete it when it is no longer needed

14. As a person whose personal data Southampton Street Pastors holds (a data subject) you have the following rights:

(a) The right to be informed of your rights as a data subject through this privacy notice.

(b) The right of access to the information Southampton Street Pastors holds on you.

(c) The right to correct the information we hold on you.

(d) The right to erase the information we hold on you.

(e) The right to restrict processing of your personal data

(f) The right to data portability and the transfer of your personal data to another data controller.

(g) The right to object to the processing of your personal data.

(h) Rights in relation to automated decision making and profiling.

15. When exercising any of the rights listed above, in order to process your request, we may need to verify your identity for your security. In such a case we may need you to verify your identity before you can exercise these rights.

16. You have the right to withdraw your consent to the processing of your personal data by Southampton Street Pastors at any time; however please note that if you withdraw your consent it may result in your being unable to continue your role within the organisation.

17. The provision of your personal data is part of a process you have entered with Southampton Street Pastors to facilitate your role within the local initiative. If you withdraw your personal data, this may result in you being unable to continue in your role.

18. Southampton Street Pastors currently has no automated decision making or profiling activities. If in future these activities are to occur, you will be notified, and your consent sought before your personal data is processed in this manner.

19. Should you be dissatisfied with the way in which the organisation has processed your data you have the right to submit a complaint to the Information Commissioner's Office:

    Information Commissioner's Office
    Wycliffe House
    Water Lane Wilmslow
    Cheshire SK9 5AF

    www.ico.org.uk/concerns/handling/

Southampton Street Pastors General Privacy Notice
How the information we hold on you will be used

1. Personal data is any information about a living individual which allows them to be identified (eg a name, email address, address, image, ID number). Identification can be by the personal data alone or in conjunction with any other information.

2. Your information/personal data will be held by Southampton Street Pastors (the local initiative). You can contact Southampton Street Pastors as a data controller and for any data protection enquires by post by writing to:

   Data Protection Officer
   Southampton Street Pastors
   [Address]

   By email at Southampton@streetpastors.org.uk and by telephone on [telephone number].

3. Southampton Street Pastors is part of a wider network of Street Pastor initiatives in the UK coming under the umbrella of Ascension Trust, a charity registered in the UK, who all work together to deliver the Street Pastors' mission in communities throughout the UK. We may need to share personal data that we hold with them so that they can carry out their responsibilities in our community. The Street Pastor network and Ascension Trust are joint data controllers and all responsible to you for how your personal data is processed. This privacy notice is sent to you by Southampton Street Pastors on our own behalf and on behalf of these other data controllers.

4. As data controllers we will comply with our legal obligations towards you to keep any personal data we hold on you up to date; to store and destroy it securely; not to collect or retain excessive or unnecessary amounts of data; to keep your personal data secure, and protect it from loss, unauthorised access, misuse and disclosure.

5. We will use your personal data for some or all of the following purposes:

   a. to enable us to deliver the Street Pastor mission to our local community, and to carry out other charitable or voluntary activities for public benefit as provided for in the governing document and statutory framework of the local initiative and its other joint controllers;

   b. to fundraise and promote our work;

   c. to send you communications which you may have requested or that may be of interest to you about our operations, events, fundraising activities, campaigns and appeals.

   d. to process a donation that you have made (including Gift Aid information);

   e. to maintain our records and accounts;

   f. to keep you notified of changes to the service that we provide, events or personnel within the local initiative;

   g. to seek your comments or views;

   h. to process applications for a role;

   i. to enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our governing document.

6. We may process the following personal data:

   a. Names, titles, aliases, photographic images.

   b. Contact details, eg telephone numbers, addresses and email addresses.

   c. Where relevant we may process demographic information such as your date of birth, marital status, nationality, family composition, dependants, education/work histories, academic/professional qualifications and employment details.

   d. Where you make donations or pay for activities or merchandise, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.

   e. Other operational personal data created, obtained, or otherwise processed in the course of the local initiative carrying out our activities including, but not limited to, recordings of telephone conversations, IP addresses and website visit histories, and logs of visitors.

   f. The data we process will likely include sensitive personal data because as a Christian organisation the fact that we process your data may be suggestive of your religious beliefs. The local initiative may also process other categories of sensitive personal data revealing racial or ethnic origin, religious or philosophical beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health.

7. Whilst we will rely on your consent as a legal basis for this processing, we will also have a legitimate interest for processing your personal data in order to facilitate the Street Pastor mission. As a religious organisation we may process information about your religious believe to administer membership or contact details. Whilst exercising our legitimate interest we will always take into account your interests, rights and freedoms.

8. Some of our processing is necessary for compliance with a legal obligation. Where your personal data is used other than in accordance with one of these legal bases, we will first obtain your consent to that use.

9. Your personal data will be treated as strictly confidential. It will only be shared with third parties including other data controllers where it is necessary for the performance of our tasks or where you first give us your prior consent.

10. We may also share your personal data with our agents, servants and contractors. For example, we may ask a commercial provider to send out newsletters on our behalf, or to maintain our database software.

11. It is not envisaged that your personal data will be transferred to any party outside of the UK, but in the event that this needs to be done, your consent will be sought beforehand. Any electronic personal data transferred to countries or territories outside the EU will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the EU. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

12. We will keep your personal data only for as long as we need it and in line with our Data Retention Policy and we will delete it when it is no longer needed. Elements of your personal data may be retained by the organisation for historical, statistical or research purposes.

13. We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 7 years to support HMRC audits.

14. As a person whose personal data Southampton Street Pastors holds (a data subject) you have the following rights:

    (i) The right to be informed of your rights as a data subject through this privacy notice.

    (j) The right of access to the information Southampton Street Pastors holds on you.

    (k) The right to correct the information we hold on you.

    (l) The right to erase the information we hold on you.

    (m) The right to restrict processing of your personal data

    (n) The right to data portability and the transfer of your personal data to another data controller.

    (o) The right to object to the processing of your personal data.

    (p) Rights in relation to automated decision making and profiling.

15. When exercising any of the rights listed above, in order to process your request, we may need to verify your identity for your security. In such a case we may need you to verify your identity before you can exercise these rights.

16. You have the right to withdraw your consent to the processing of your personal data by Southampton Street Pastors at any time.

17. Southampton Street Pastors currently has no automated decision making or profiling activities. If in future these activities are to occur, you will be notified, and your consent sought before your personal data is processed in this manner.

18. Should you be dissatisfied with the way in which the organisation has processed your data you have the right to submit a complaint to the Information Commissioner's Office:

    Information Commissioner's Office
    Wycliffe House
    Water Lane Wilmslow
    Cheshire SK9 5AF

    www.ico.org.uk/concerns/handling/

SCHEDULE 3
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 written 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 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. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

6. If requested, the local initiative must 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. Where possible compliance should be done electronically by email.

7. 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.

8. 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.

9. Information must 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.

10. 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.

11. 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.

    Reasons for refusal can include confidentiality in certain circumstances, eg where a less than favourable reference has been provided for an individual applying to become a Street Pastor and the referee has asked that the reference be kept confidential and not disclosed to the applicant. If the reference results in the application being rejected, the specific reason for the rejection should not be disclosed to the applicant, as this might identify the cause of the rejection. If necessary, advice should be sought from Ascension Trust's Legal & Policy Officer on how to respond.

12. 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.

13. If the request is made electronically, the local initiative should provide the information in a commonly used electronic format, eg by email.

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

15. 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 be redacted.

16. The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to their information, eg via a secure Dropbox link to a file containing their information.

17. The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

18. 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 would generally carry with them a duty of confidence in relation to information disclosed.

- Pastoral (minister and member of their congregation, eg 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.

19. 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, eg "Any personal data related to the decision to discipline me and the subsequent disciplinary proceedings."

20. 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.

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

SCHEDULE 4
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, Southampton 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 (eg 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 any body 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.

9. DBS logo

The DBS logo is protected by crown copyright, the copying and use of the DBS logo is not permitted without prior approval of the DBS.

10. Disclosure and Barring Service

DBS customer services
PO Box 3961
Royal Wootton Bassett
SN4 4HF

customerservices@dbs.gsi.gov.uk

DBS helpline: 03000 200 190