DATA PROTECTION AND INFORMATION SECURITY POLICY

Data Protection Policy

for South Eastern Baptist Association

July 2024

V1.1

Table of Contents

Introduction

The Data Protection Act 2018 (DPA) and the UK GDPR is the law that protects personal privacy and upholds individuals' (sometimes referred to as 'data subjects') rights. It applies to anyone who handles or has access to people's personal data.

This Policy is intended to ensure that personal information is dealt with properly and securely and processed in accordance with the DPA and the UK GDPR. It applies to personal information regardless of the way it is used, recorded or stored and whether it is held in paper files or electronically. It sets out the roles and responsibilities of the South Eastern Baptist Association (SEBA or 'the Association') and its team in relation to information security and data protection, and the process by which breaches will be investigated.

This Policy also covers records held by the Association which do not contain personal data in the meaning of the Act but remain sensitive or confidential.

The Policy applies to all colleagues including Ministers, employed staff, volunteers, contractors and Trustees. All users of Association data are responsible for the information they use, create, process, access and transfer. All forms of data and information are included in this policy:

- electronically held data, regardless of storage media and including information in the cloud (e.g. Microsoft 365, SharePoint etc.) as well as on individual computers, laptops or on mobile devices;
- paper based information (including notebooks and temporary records);
- information derived from any business process, regardless of the storage or system;
- all other data; both internally produced or obtained from other bodies

Legal consequences

This Policy complies with the requirements of the Data Protection Act 2018 and the UK GDPR.

Policy

The South Eastern Baptist Association is a data controller registered with the Information Commissioner's Office (ICO) with registration number Z2441527.

The Association will comply with its obligations under the DPA and the UK GDPR. The Association is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure that its colleagues, members and partner organisations are aware of their rights under the legislation through the publication of clear and transparent privacy notices.

The Association processes personal data to enable it to, amongst other purposes:

- Provide a voluntary service for the benefits of the public in Great Britain;
- Administer membership records;
- Fundraise and promote the interests of the charity;
- Manage our employees and volunteers;
- Maintain our own accounts and records.

The Association will protect its information by adopting a range of measures to act against possible security threats, whether internal or external, deliberate or accidental. The implementation of this policy is important to maintain the integrity of our information, to meet information access legislation requirements, and to protect our reputation.

All colleagues must have a general understanding of the law and in particular, know how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All colleagues must understand and comply with this policy and undertake any learning as directed by the Association.

Purpose and aims of the policy

The purpose of information security and data protection is to provide an appropriate level of protection for information assets (data) from possible threats, whether internal or external, deliberate or accidental.

The Association is dependent on information and its availability. The Association holds and processes data which may be sensitive or be important information in supporting business processes and services to our members, and in conforming to legal and statutory requirements. The DPA requires information to be protected in line with individuals' rights, and in consideration of individuals privacy.

The Association aims to identify risks to data security, in terms of loss of confidentiality, integrity and availability, and adopt appropriate measures to protect information from unauthorised or accidental modification, loss, or inappropriate release or use. These measures will include a range of procedures and organisational and technological measures, to a level commensurate with the identifiable risks and the information's value to the Association.

We do not hold information relating to criminal proceedings or offences or allegations of offences other than in the specific circumstances set out in this policy.

'Personal data' is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the data. The data includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the UK GDPR personal data also includes an identifier such as a name, an identification number, location data or an online identifier.

The Association collects and uses personal data for a number of specific lawful purposes as set out in detail in its privacy notice(s) and in Schedule 2. These include carrying out its business and fulfilling its role as a Charity. Data is held on past, current and prospective colleagues, members, suppliers and others with whom we communicate.

Correct and lawful treatment of personal data will maintain confidence in the Association. Protecting the confidentiality and integrity of personal information is critical.

Roles and responsibilities

The overarching responsibility for Information Security and Data Protection rests with the Trustees of the Association. The Trustees delegate day-to-day responsibility to the Operations Manager in their role as the Data Protection Officer (DPO) for the Association.

The Association will allow the DPO to act independently, provide adequate resources to enable them to fulfil the role effectively and report to the highest level of management.

The Association will follow advice provided by the DPO and document any reasons why, by exception, it decides not to follow such advice.

The DPO is tasked with ensuring compliance with data protection law, dealing with data security breaches and with the development of this policy. However, the DPO will not be personally liable for any breach of the DPA or UK GDPR and ultimate responsibility for compliance with the DPA and UK GDPR remains with the Trustees of the Association, as the data controller. Nevertheless, the DPO clearly plays a crucial role in helping the Association to fulfil its protection obligations.

The Operations Manager will:

- Hold the position of Data Protection Officer. The DPO is a member of the senior management board of an organisation with overall responsibility for an organisation's information risk policy. The DPO is accountable and responsible for information risk across the Association.
- Monitor compliance with the UK GDPR and other data protection laws, our data protection policies, raise awareness, conduct training and audits;
- Provide advice and information to the Association on its data protection obligations as described in Article 39;
- Advise on, and to monitor, data protection impact assessments;
- Act as a contact point for the Information Commissioners Office (ICO) and fully co-operate with the ICS, including prior consultations under Article 36, and will consult on other matters;
- When performing tasks, have due regard to the risk associated with data processing operations, and take account the nature, scope, context and purpose of processing;
- Act as the point of contact for the Association’s colleagues, its members, partners and the public, including people whose personal information is being processed;
- Seek advice as required;
- Prioritise and focus on the more risky activities, for example where special category data is processed, or where the potential impact on individuals could be damaging. The DPO, will provide risk-based information to the Association;
- Maintain and publish a data retention schedule setting out what data is held and how long it should be retained for;
- Implement and maintain a process for identifying, and investigating potential breaches of the Association’s data security, including near misses;
- Respond to and lead the resolution of any information security incidents. Keep a record of and, if necessary, report any potential security breaches to the ICO.
- Authorise the release of data held by the Association to any third party;
- Complete Privacy Impact Assessments where significant quantities of data\information are received or where new systems that will process personal data are implemented.
- Co-ordinate and advise on any data sharing protocols and related information security implications.

- Implement appropriate technological measures to ensure the security of data capture, data integrity and data access on servers/systems and within their span of control.
- Advise and support the Association to implement any further technological measures for specific systems, particularly in relation to data transfer, data sharing, disposal of equipment, and access to data. This may include encryption and security of mobile devices.
- Ensure that contracts entered into by the Association give appropriate consideration to the processing and protection of any data passed to or from the Association, including personal data and special category data, including how it is processed by the contracting party, where it is stored and how it is destroyed when no longer relevant, or when the contract ends.
- Provide or arrange training and guidance for the trustees of the Association and members of staff.
- Keep the content and effectiveness of this policy under review and oversee compliance with this policy.

All colleagues will:

- Comply with the information security and data protection policy and associated procedures, and play an active role in protecting the Association's information. Colleagues must not access or process information without authorisation to do so. All colleagues must report security breaches, data incidents or exposures coming to their attention to the DPO.
- Keep data secure, this includes personal data and special category data. Any hard copy personal data (e.g. operational, financial, commercial, organisational) must be reasonably secure when not in use and must not be left out on display. The Association accepts that data kept at home is 'reasonably secure' provided the colleagues are not careless or negligent with the data. Data must not be kept in unsecured vehicles or any vehicle overnight. Data must be kept secure when visiting churches or other public spaces.
- Lock their computer screens whenever they leave their computer unattended in spaces where there are other people. This includes instances such as when leaving the computer within a church building or public space.
- Comply with and not attempt to circumvent the administrative, physical and technical safeguards the Association has implemented and maintains in accordance with the UKGDPR.
- Take personal responsibility for computers, hardware and mobile devices that may contain Association data – ensuring software on such devices is kept up to date to maintain security.
- Ensure they are reasonably aware of their responsibilities under the DA and the UK GDPR and comply with the principles relating to the processing of personal information, in particular if they handle personal data regularly in the course of their duties. All colleagues must complete any training relevant to this policy when requested to do so.
- Surrender or destroy all Association data, as requested, when they leave the employment or voluntary role for the Association.

The Principles

The principles set out in the UK GDPR must be adhered to when processing personal information (referred to in the UK GDPR as 'personal data'). The data protection principles set out below are applicable across the Association.

- Personal data must be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
- Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed ('data minimisation').
- Colleagues may only process personal information when their role requires it. Colleagues must not process personal information for any reason unrelated to their role.
- Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay ('accuracy').
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data is processed ('storage limitation')
- Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal data are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data ('integrity and confidentiality')

Transfer limitation

Personal information shall not be transferred outside the United Kingdom (UK) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information as determined by the UK GDPR or where the organisation receiving the personal information has provided adequate safeguards. This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer personal information where the data subject has provided explicit consent or for other limited reasons. Colleagues should contact the DPO if they require further assistance with a proposed transfer of personal information.

Lawful basis for processing personal information

Before any processing activity starts for the first time, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be approved by the DPO to ensure that at least one of the following conditions listed in Article 6 of the UK GDPR is satisfied:

- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the Association is subject;
- processing is necessary for the purposes of the legitimate interests pursued by the Association or by a third party;
- the data subject has given consent to the processing of his or her personal information for one or more specific purposes.

    - Consent should generally be seen as the last resort where no other lawful basis exists. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters. Where consent is relied on, data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. New consent will need to be obtained if personal information is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

Colleagues must be satisfied that the processing is necessary for the purpose of the relevant lawful basis (and that there is no other reasonable way to achieve that purpose).

The decision as to which lawful bases or basis applies must be documented, to demonstrate compliance with the data protection principles. Information must be provided about both the purpose(s) of the processing and the lawful basis for it in the Association's relevant privacy notice(s).

Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Special categories of personal data

Processing of sensitive personal information (known as 'special categories of personal data' in the UK GDPR) is prohibited unless a lawful special condition for processing is identified.

Special category personal data is information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, concerns health, a person's sex life or sexual orientation or is genetic or biometric data which uniquely identifies a natural person. Clearly religion is very likely to be recorded by the Association.

Special category personal information will only be processed if there is a lawful basis for doing and one of the special conditions for processing special category personal information applies. Advice is to be sought from the Operations Manager if special category data has to be processed by the Association.

The Association's privacy notice(s) set out the types of special category personal information that it processes, what it is used for, the lawful basis for the processing and any exceptions or conditions that are relied upon.

Special category personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Where explicit consent is required for processing special category personal information, evidence of consent will need to be captured and recorded so that the Association can demonstrate its compliance with the law.

Special category or criminal convictions etc data ("criminal offence data") may also be processed by the Association where it fulfils one of the substantial public interest conditions under Schedule 1, Part 2 of the Data Protection Act 2018, in particular, Conditions 10, 11, 12, 18 and 19.

The Association may also seek to obtain, use and retain criminal offence data in reliance upon Condition 31 relating to criminal convictions under Schedule 1, Part 3 of the Data Protection Act 2018.

For the purposes of Schedule 1, Part 4 of the Data Protection Act 2018, more information about the Association's processing of special category and criminal offence data under Conditions 10, 11, 12, 18, 19 and 31 found in the "Appropriate Policy Document" in Schedule 2 of this policy.

Automated decision making

The Association does not use automated decision-making in any of its data processing.

Data Protection Impact Assessments

All data controllers are required to implement 'Privacy by Design' when processing personal information. This means the Association's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles (such as data minimisation).

Where processing is likely to result in high risk to an individual's rights and freedoms (for example where a new technology is being implemented or if it will involve large-scale processing of special category data or information relating to criminal offences) a data protection impact assessment must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Colleagues should seek the advice of the DPO as to whether a data protection impact assessment needs to be referred to the Information Commissioner's Office As part of their Data Protection Officer, the DPO will sign off the data protection impact assessment as suitable and sufficient at the appropriate point.

Documentation and records

Written records of processing activities that involve large volumes of data or special category data or must be kept and should include:

- the name of colleague(s) carrying out the processing
- the purposes of the processing
- the lawful basis for the processing
- a description of the categories of individuals and categories of personal data
- whether personal information of children is being processed
- details of the recipients of personal information
- where relevant, details of transfers to countries outside of the European Economic Area or to international organisations, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures in place.

As part of The Association's record of processing activities the DPO will document, or link to documentation, on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information
- data protection impact assessments and
- records of data incidents and confirmed data breaches.

Records of processing of special category personal information are kept on:

- the relevant purposes for which the processing takes place, including why it is necessary for that purpose
- the lawful basis for our processing and
- whether the personal information is retained or erased in accordance with The Association's Data Retention Scheme and, if not, the reasons why.

Privacy notices

The Association will issue or publish privacy notices from time to time as required, informing individuals about the personal information that it collects and holds and details of how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from individuals, including for Human Resources or employment purposes, the individual shall be given all the information required by the UK GDPR including the identity of the data controller and the Data Protection Officer, how and why the Association will use, process, disclose, protect and retain that personal information.

When information is collected indirectly (for example from a third party or publicly available source) the individual must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the personal information and no later than one

month from that date. Data collected by a third party must also be obtained in accordance with the UK GDPR and used in a way that is consistent with the proposed use of the personal information set out in the privacy notice.

The Association will take appropriate measures to provide information in privacy notices in a concise, transparent and easily accessible form, using clear and plain language.

Storage limitation

The Association maintains a Data Retention Schedule, at **Appendix 1**, to ensure personal information is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such personal information to be kept for longer. Colleagues must take all reasonable steps to destroy or delete from the Association's systems, including computer drives, paper records and mobile devices, all personal information that is no longer required in accordance with the Schedule. This includes requiring third parties to delete such personal information where applicable.

The Association will inform individuals of the period for which personal information is stored and how that period is determined in any applicable privacy notice.

Individual rights

All 'data subjects' rights in relation to their personal information as detailed in Schedule 1 and summarised below:

- to be informed about how, why and on what basis that information is processed (see the Association's privacy notice(s))
- confirmation that personal information is being processed and to obtain access to it and certain other information, via a subject access request
- to have personal information corrected if it is inaccurate or incomplete
- to have personal information erased if it is no longer necessary for the purpose for which it was originally collected/processed or when the consent on which the processing is based has been withdrawn and there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful or where the personal information is no longer needed by the Association but the individual requires it to establish, exercise or defend a legal claim, and
- to restrict the processing of personal information temporarily where an individual does not think it is accurate (and the Association is verifying whether it is accurate), or where an individual has objected to the processing (and the Association is considering whether its legitimate grounds override an individual's interests)
- in limited circumstances to receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine readable format
- where processing of personal information is based on consent, to withdraw that consent at any time
- to request a copy of an agreement under which personal information is transferred outside of the European Economic Area
- to object to decisions based solely on automated processing, including profiling

- to be notified of a data breach which is likely to result in high risk to their rights and obligations
- to make a complaint to the Information Commissioner's Office or a Court

Anyone wishing to exercise any of the rights above, or who receives a request from someone else to exercise any of the rights above, should contact the Operations Manager for advice.

Individual responsibilities

Individuals are responsible for helping the Association keep their own personal information up to date. Colleagues must inform the Operations Manager or Association Administrator if their personal information changes, for example if they move home.

Colleagues may have access to the personal information of other colleagues, suppliers, members or the public in the course of their employment or volunteering for the Association. If so, the Association expects colleagues to help meets its data protection obligations to those individuals. For example, colleagues should be aware that those individuals enjoy the rights set out above.

If colleagues have access to personal information, or any other form of sensitive, but not personal data or information, they must:

- only access the information that they have authority to access, and only for authorised purposes
- only allow other colleagues to access information if they have appropriate authorisation
- only allow individuals who are not colleagues to access information if they have specific authority to do so
- keep information secure (e.g. access to premises, computer access, password protection and secure file storage and destruction)
- not remove information, or devices containing personal information (or which can be used to access it) from premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store information on local drives or on personal devices
- comply with the destruction periods set out in the Association's Data Retention Schedule
- destroy redundant information in an appropriate way, e.g. shredding of paper records

Security requirements

Security is a requirement under the Data Protection Act 2018, and may additionally be contractually required by other organisations, particularly where data sharing operates. Actions are taken by the Association to ensure information security from a technology perspective by means of passwords, firewalls and back-ups for example. The DPO provides guidance and monitoring for processes and standards.

Colleagues must follow all policies and guidance, and where necessary, in liaison with the DPO, adopt any additional security commensurate with the nature, value and risk to the data. This applies to personal data as well as any other records held by the Association which are not personal data but remain sensitive.

The measures implemented must be an appropriate package of technology, process and organisational controls, and ensure the information is protected throughout the life cycle of the information from creation to processing, storage and disposal.

As a minimum, specific security measures must be applied which ensure that:

- information is valued, then the security of the information risk assessed, and appropriate controls implemented Unauthorized access is prevented
- confidentiality is maintained
- unauthorised disclosure through deliberate or careless action is prevented
- integrity of information is assured by preventing unauthorized modification
- information is accessible to authorised users
- regulatory and legislative requirements are met
- business continuity plans for ensuring information availability are produced, maintained and tested as far as practicable
- information security guidance is available for colleagues
- all suspected breaches of information security are reported to the DPO and then investigated.
- all agreements relating to information and data sharing protocols must include a section detailing security requirements

Data breaches

A data breach may take many different forms:

- loss or theft of data or equipment on which personal information is stored
- unauthorised access to or use of personal information either by a member of colleagues or third party
- loss of data resulting from an equipment or systems (including hardware or software) failure
- human error, such as accidental deletion or alteration of data or emailing the wrong individual or pressing ‘reply all’ instead of ‘reply’
- unforeseen circumstances, such as a fire or flood
- deliberate attacks on information technology systems, such as hacking, viruses or phishing scams
- blagging offences where information is obtained by deceiving the organisation which holds it

If the Association becomes aware of a data breach that is likely to result in a risk to individuals’ rights, it must report it to the Information Commissioner’s Office within 72 hours (where possible), but in any event, without undue delay. The Association will also notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

Colleagues must inform the DPO immediately if a data breach is discovered and make all reasonable efforts to recover any information.

Training

The Association will ensure that colleagues are adequately trained regarding their data protection responsibilities. All colleagues are required to complete information governance and data protection training every two years as a minimum or as requested by the DPO.

Data sharing

Any regular sharing of data between the Association and third parties will require an information sharing agreement.

Consequences of a failure to comply

The Association takes compliance with this policy very seriously. Failure to comply puts data subjects at risk and carries the risk of significant civil and criminal sanctions for the individuals responsible and for the Association and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action.

If colleagues have any questions or concerns about this policy they should contact the Operations Manager.

Schedule 1 - Rights of data subjects

Under the UK GDPR data subjects have various rights. These are described below.

Please note that the descriptions below are only intended to be used as guidance and do not, in any way, affect how they apply under the UK GDPR. We will apply the rights in accordance with the UK GDPR which overrides the text of this schedule.

Those who wish to obtain more information about this procedure or their data protection rights generally may contact our Data Protection Officer:

South Eastern Baptist Association

17 Cherry Close

Burgess Hill

RH15 9PR

Tel: 01444 233431

Email: dataprotection@seba-baptist.org.uk

Right of Access

Data subjects have a right to access personal data about them which we hold. It is not a right to documents, but only to personal data contained in documents. This does not cover personal data which relates to other persons.

Under the UK GDPR, requests must be complied with without undue delay and, in any event, within one calendar month from the date of receipt of the request. This time limit can be extended by two months where necessary, taking into account the complexity and number of requests. For an extension to apply the data subject must be informed of the extension and why it is needed within one month of the request.

If the request is made electronically, the information should be provided in a commonly used electronic form.

If more than one copy of the data is requested, we may charge a reasonable fee based on our administrative costs for providing the extra copies. If a request is manifestly unfounded or excessive, we are entitled to refuse to comply with the request or to charge a reasonable fee (based on administrative costs) to deal with the request. We must inform the data subject about this and explain to the data subject that they have a right to complain to the ICO. We will not apply this exception unless we have a strong justification to do so.

Right to Rectification

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

Right to Erasure (to be forgotten)

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

- it is no longer needed;
- the only legal ground for processing is consent and the data subject withdraws consent;
- the data subject objects to processing (see the Right to Object below) and there are no overriding legitimate grounds to continue with the processing;
- the data has been processed unlawfully;
- the data has to be erased for compliance with a legal obligation which applies to us.

There are exceptions to this right. These include when processing is required for compliance with the law, reasons of public interest, research or statistics, and legal claims.

Right to Restrict Processing

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

- if the accuracy of the data is contested, for a period which enables us to verify the accuracy of the data;
- if the processing is unlawful and the data subject opposes the erasure of the data but requests restriction of its use instead;
- if we no longer require the data but the data subject needs the data for the establishment, exercise or defence of legal claims;
- the data subject has objected to data processing (see the Right to Object below), until an assessment is made of whether there are overriding legitimate grounds which can justify the continuation of the processing.

Even if the data subject exercises this right we are entitled to process the data in question for purposes relating to legal claims, for the protection of the rights of other persons or for reasons of public interest.

We must inform the data subject when the restriction will be lifted.

Right to Object

Where data is processed for the performance of a task carried out in the public interest or legitimate interests pursued by us or a third party, data subjects may object to the processing on grounds relating to their particular situation. In such a case, we will stop processing that data unless there are compelling legitimate grounds for the processing to continue or if the processing is required in connection with legal claims.

Data subjects can object to the processing of their data for purposes of direct marketing. This is an absolute right and the processing should cease on request.

When data is processed for research or statistical purposes, data subjects can object on grounds relating to their particular circumstances, unless the processing is required for reasons of public interest.

Right of Data Portability

Data subjects have a right to receive personal data which they provide to us in a structured, commonly-used, and machine-readable (digital) format and are entitled to transmit that data to any other person if the processing of that data is carried out by automated means and is based on 1. the data subject's consent or 2. is processed out of necessity for the purpose of performing a contract with the data subject. Data subjects may also request that we transfer their data directly to a third party.

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

Other Rights

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

- To be provided with privacy notices;
- To request information about persons to whom their personal data has been disclosed;
- To withdraw consent to processing which is based on consent. Withdrawing consent should be as easy as it is to give consent. Withdrawal of consent does not affect the lawfulness of processing already carried out;
- To make a complaint to the Information Commissioner's Office (https://ico.org.uk/);

Not to be subject to decisions based solely on automated data processing which significantly affect them or which produce legal effects concerning them.

Exercising rights

Data subjects who wish to exercise any of the above rights or who have any questions about them should contact our Data Protection Officer whose contact details are at the top of this Schedule.

Any information provided to data subjects should be provided in a concise, transparent, intelligible and clearly accessible form, using clear and plain language.

We are required to provide information on action taken subsequent to a request by a data subject based on the above rights, without undue delay and within one month from when we receive the request. This can be extended by two further months where necessary,

depending on the complexity and number of requests. If an extension is required we must inform the data subject within one month of receiving the request and give reasons for the delay.

We may refuse to comply with requests that are manifestly unfounded or excessive or, alternatively, we may charge a reasonable charge based on our administrative costs. If no action is to be taken, the data subject must be informed of that fact and the reasons within one month from the date of the request. The data subject must also be informed of their right to make a complaint to the ICO.

If a request is made by electronic means, all information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Schedule 2

Appropriate Policy Document – South Eastern Baptist Association

Schedule 1, Part 4, Data Protection Act 2018: processing of special category and criminal offence data for the purposes of Parts 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018.

Who we are

The South Eastern Baptist Association (SEBA) is an association of around 150 churches across Kent, Sussex, Surrey and a small part of North East Hampshire. We are a registered charity and part of Baptist Together, a wider organisation representing the Baptist family and the Baptist Union of Great Britain.

For further information on what we do, please visit our website: www.seba-baptist.org.uk

What this policy does

This policy explains how and why the SEBA collects, processes and shares special category personal data about you and data relating to criminal convictions etc in order to carry out our functions, in accordance with the data protection principles set out in the Retained General Data Protection Regulation (UK GDPR.) Pursuant to Part 4 of Schedule 1 of the Data Protection Act 2018 (DPA 2018), special category data (Parts 1 and 2 of Schedule 1), and data relating to criminal convictions etc (Part 3 of Schedule 1), can only be processed lawfully if it is carried out in accordance with this policy. SEBA staff and workers must therefore have regard to this policy when carrying out sensitive processing on behalf of the SEBA.

Our approach to data protection

SEBA is committed to an information assurance and data governance framework that is clear and accessible and which ensures that the collection and processing of personal data is carried out in accordance with the UK GDPR and the DPA 2018.

This is underpinned and implemented throughout the Union through the provision of training for all staff on data protection to ensure compliance with our policies and procedures and through the provision of legal advice and template documentation for member churches and associations in the wider Baptist family.

SEBA values openness and transparency, and we have committed to and published a number of policies and processes to assist data subjects and to explain how we handle personal data. These include the SEBA data protection policy, SEBA data retention schedule (Appendix 1) and the privacy statements on our website (www.seba-baptist.org.uk/User/PrivacyPolicy.aspx) which describe what information we hold, why we hold it, the legal basis for holding it, who we share it with, and the period we will hold it for.

SEBA has appointed a Data Protection Officer (DPO), who is the Operations Manager for the Association. The DPO has the day to day responsibility for ensuring that the information the Union collects is necessary for the purposes required and is not kept in a manner that

can identify the individual any longer than necessary. The DPO reports to the Team Leader and provides a legal update to the charity trustees. Data protection training is provided by the DPO for all new staff to ensure that all colleagues are familiar with SEBA's data protection policies and procedures. Particular attention is given to the Operations Team and Regional Ministers, who may be required to process special category and criminal offence data. The DPO reviews the Data Protection Impact Assessments for these teams regularly.

Due to the nature of the work performed by SEBA, the Association often needs to share information with other organisations and third parties. SEBA has Data Sharing Agreements that govern the transfer of information between us and our partner organisations such as the Baptist Union of Great Britain (BUGB).

The data protection principles

In summary, Article 5 of the UK GDPR states that personal data shall be:

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary, and
- kept secure

Special category data and criminal convictions etc data

Special category data

Personal data refers to any information by which a living individual can be identified. Individual identification can be by information alone or in conjunction with other information. Certain categories of personal data have additional legal protections when being processed. These categories are referred to in the legislation as "special category data" and are data concerning:

- health
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- sex life or sexual orientation

Criminal convictions etc data

The processing of criminal convictions etc data also has additional legal safeguards. Criminal convictions etc data ("criminal offence data") includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

Special category and criminal offence data we process about you

SEBA collects, processes and shares special category and criminal convictions data where it is necessary in order to carry out our functions. This processing is usually carried out by the Safeguarding Lead, Operations Team and Regional Ministers and is processed for the purpose of safeguarding against any risks posed to others by those who work in Baptist ministry or are involved in Baptist churches, to mitigate the risk of individuals committing criminal offences (including of a sexual nature) and to assess individuals' suitability for ministry or other work within the Baptist Union, including by reference to risks they may pose to others. These functions and the requisite processing of personal data are matters of substantial public interest.

If we process personal information about you, you are a "data subject." Below is a non-exhaustive list of categories of data subjects who we might process information about:

- Employees, volunteers, workers or charity trustees of SEBA;
- A child or individual in membership with or associated with a Baptist church or organisation in membership with SEBA;
- Individuals in Baptist ministry including BUGB accredited ministers, church workers, recognised preachers, pastors or pioneers, applicants for ministry and those previously accredited or recognised for ministry by BUGB.

SEBA will share this data with third parties only where strictly necessary (please see the section "Who we share your personal data with" below).

Special category data and criminal offence data may be collected from the following non-exhaustive list of sources:

- Data subjects
- Member Churches – usually ministers, church officers, workers or volunteers, most commonly the minister or church's Designated Person for Safeguarding
- BUGB Specialist Teams
- Police, Social Services or the Local Authority Designated Officer for safeguarding

SEBA may also obtain and process this data for other statutory and legal obligations for example, including, but not limited to:

- responding to data subject access requests under data protection legislation
- in connection with our duties under the Equality Act 2010.

The legal basis for processing your special category or criminal convictions data

The legal bases for our processing of special category and criminal offence data is Article 6(1)(f) UK GDPR and Conditions 10, 11, 12, 18, 19 and 31 of Schedule 1 Data Protection Act 2018, which are described below:

Article 6(1)(f) UK GDPR, where the processing is necessary for the purposes of the legitimate interests of SEBA, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special category or criminal offence data may also be processed by SEBA where it fulfils one of the substantial public interest conditions under Schedule 1, Part 2 of the Data Protection Act 2018:

Condition 10:

where the processing is necessary for the purposes of the prevention or detection of an unlawful act, it must be carried out without the consent of the data subject so as not to prejudice those purposes, and is necessary for reasons of substantial public interest.

In order to mitigate the risk of individuals committing criminal offences, including of a sexual nature, the Union may undertake a risk assessment on an individual who has been reported to us by another individual or a statutory authority, where there is a significant concern about their conduct and the risk they may pose to others.

Condition 11:

where the processing is necessary for the exercise of a protective function, it must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and is necessary for reasons of substantial public interest. In this paragraph, "protective function" means a function which is intended to protect members of the public against – dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence, mismanagement in the administration of a body or association, or failures in services provided by a body or association.

SEBA exercises protective functions through the work of its Safeguarding and Ministries Teams, which include assessing individuals' suitability for ministry or other work within the Baptist family, including by reference to risks they may pose to others. SEBA discharges these functions by custom, practice and with the consensus of member churches and the requisite processing of personal data is a matter of substantial public interest.

Condition 12:

where the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct, and in the circumstances the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and the processing is necessary for reasons of substantial public interest.

SEBA may assist BUGB to investigate and risk assess an individual's suitability for ministry or other work within the Baptist family and refer to the Ministerial Recognition Committee or a MRC sub-committee, for the purposes of safeguarding, ministerial accreditation and its disciplinary process in relation to ministerial recognition, which is in the substantial public interest and forms an integral part of "generally accepted principles of good practice" as per the definition of "regulatory requirement" in Condition 12.

Condition 18:

where the processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, the individual is - aged under 18, or aged 18 and over and at risk, the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and (d) the processing is necessary for reasons of substantial public interest. (2) The reasons mentioned in sub-paragraph (1)(c) are – (a) in the circumstances, consent to the processing cannot be given by the data subject; (b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing; (c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

SEBA processes criminal and special category data for the purposes of safeguarding minors and vulnerable persons or adults at risk.

Condition 19:

where the processing is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 and over and the processing is of data concerning health, is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and is necessary for reasons of substantial public interest. An “individual at economic risk” means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability.

SEBA may seek to rely on this condition if it is required to assist BUGB to investigate allegations of financial abuse by an individual in ministry or other work within the Baptist family for the purpose of safeguarding vulnerable persons or adults at risk.

SEBA may also seek to obtain, use and retain criminal offence data in reliance upon the following additional condition relating to criminal convictions under Schedule 1, Part 3 of the Data Protection Act 2018:

Condition 31:

where the processing is carried out by a not-for-profit body with a religious aim in the course of its legitimate activities with appropriate safeguards where it relates solely to the members or former members of the body or to persons in regular contact with it in connection with its purposes, and the personal data is not disclosed outside that body without the consent of the data subjects.

Policy Owner	Operations Manager
Date Issued	09/07/2024

Version	Revisions	Date Approved
V1.0	New standalone policy (previously part of staff handbook)	08/07/2024
V1.1	Data retention schedule updated to show correspondence only kept for five years as confirmed	02/12/2024

Appendix 1

Data Retention Schedule

Introduction

This record retention schedule accompanies the South Eastern Baptist Association Data Protection Policy and has been adopted in compliance with the storage limitation principle in the Retained General Data Protection Regulation (UK GDPR). It sets out the time periods that different types of documents and records must be retained for business and legal purposes. This is a lengthy document listing the many types of records used by the Association and the applicable retention periods for each record type.

The retention periods are based on business needs and legal requirements. Information which is held longer than necessary carries additional risk and cost. Retention periods are independent of format and can therefore be applied to any medium whether paper or electronic. Data retention periods are listed below but please note that some software systems used by the Association may retain data for a limited period after being deleted before it is irretrievable .

This policy applies to all colleagues and workers who process personal data in their role within the Association.

Contents

Employment/HR	All information relating to recruitment, selection and development whilst in post	6 years after post-holder has left the Association's employment	Limitation Act 1980 (1)	Destroy
	Information on any disciplinary or grievance matter that is still 'live' on the individual's personnel file,	6 years after post-holder has left employment	Limitation Act 1980 (1)	Destroy

	including information on any penalty or warning imposed			
	Information on an individual's health and sickness record, including information on any adjustment made to their working pattern, either on a temporary or permanent basis	6 years after post-holder has left employment	Limitation Act 1980 (1)	Destroy
	Redundancy records	6 years from date of redundancy	Limitation Act 1980	Destroy
	Information on any safeguarding concern or matter in which the employee was involved in any way	75 years after employment/role ceases (see Safeguarding Retention Schedule below)	Requirements of the Independent Inquiry into Child Sexual Abuse (IICSA)	Not applicable
	Record of a Disclosure and Barring Service (DBS) check being undertaken for a Minister or other SEBA worker (paid or voluntary)	75 years after employment / role ceases or 75 years after the death of a minister (see RUGB guide to DBS checks)	To allow investigation into any future allegations	Destroy
	Parental leave records	18 years from the date of the birth of a child	To enable future employers to check entitlement	Destroy
	Payroll records including correspondence with HMRC (2)	6 years from the end of the financial year the records relate to.	Charities Act and HMRC Rules	Destroy
	Pensions Records	According to the schedules set by the Pension provider		Destroy

	Application forms and interview notes for unsuccessful candidate	6 months to a year	2010 Equality Act recommends six months. One year limitation for defamation actions under Limitation Act.	Destroy

	Complaints records	1 year where complaint referred elsewhere otherwise 6 years from last action	Limitation Act 1980	Destroy

1. *Six years is generally the time limit within which proceedings founded on contract may be brought*
2. *Note that the Association has outsources it's payroll function and therefore most records are retained by it's payroll provider.*

Finance	All financial records – invoices, bills, bank statements, paying in books etc	6 years from the end of the financial year the record relates to	Charities Act and HMRC Rules	Destroy
	Gift Aid declarations	6 years after the last payment was made	HMRC Rules	Destroy
	Legacy information (i.e. documents which relate to a legacy received by the Association)	6 years after the deceased's estate has been wound up	In line with requirements for other financial information	Destroy
	Annual Accounts and Reports	10 years [3]	Good practice	Archive (e.g. County Archive Office)
	Payroll records including correspondence with HMRC [2]	See Employment/HR above	See Employment/HR above	See Employment/HR above

3. *These should be kept permanently somewhere. 10 years is the suggested minimum period the information is held by the Association before sent to archives.*

General	Correspondence (including emails)	Unless this relates to any other category of data listed here (e.g. finance, employment, safeguarding etc) correspondence will only be kept for as long as is relevant. By default, emails will be kept for 5 years and then destroyed.

Health and Safety	Reportable accidents / accident book	3 years after date of entry or end of any investigation if later	The Reporting of Injuries, Diseases and Dangerous	Destroy

			Occurrences Regulations 2013	
	Records documenting external inspections	3 years after date of inspection	Good practice	Destroy

Insurance	Public liability policies and certificates	Permanently	Historical claims/commercial practice	Store securely with electronic copy as backup
	Employer's liability policies	Permanently	Employers' Liability (Compulsory Insurance) Regulations 1998 suggests 40 years	Store securely with electronic copy as backup
	Sundry insurance policies and insurance schedules	Until claims under policy are barred or 6 years after policy lapses, whichever is longer	Commercial practice	Destroy
	Claims correspondence	6 years after last action	Commercial practice	Destroy

Meetings	Trustee and Finance Meeting Minutes	10 years min from the date of the meeting [4]	Good practice	Archive (e.g. County Archive Office)
	Leadership Meeting Minutes	5 years from the date of the meeting	Good practice	Archive (e.g. County Archive Office)
	Minutes of internal groups	3 years from the date of the meeting	Good practice	Destroy unless of particular value in which case send to Archive

4. *These should be kept permanently somewhere. 10 years is the suggested minimum period the information is held by the Association before sent to archives.*

Membership	Membership List (Names)	Permanent but reviewed and updated regularly	Good practice	
	Contact details of Members	Kept up to date. Out of date contact details not retained	Good practice	Destroy

Property	Title Deeds for property (where Association holds their own)	Permanently or until property is disposed of	Limitation Act 1980	Keep copy for 6 years after property has been disposed of
	Leases	12 years after lease and liabilities under the lease have terminated	Limitation Act 1980	Destroy
	Final plans, designs and drawings of the building, planning consents, building certifications, collateral warranties, records of major refurbishments and redevelopments.	Permanently or until six years after property is disposed of	Limitation Act 1980	Destroy 6 years after property is disposed of

Safeguarding	Safeguarding records will be retained in accordance with recommendations from Baptists Together see www.baptist.org.uk/gdprsafeguarding	75 years or more	Various, refer to separate guidance	Destroy

Website and communications platforms	The website makes use of YouTube, Zoom and Microsoft Teams for playing videos, webinars and live broadcasting. It also makes use of Buzzsprout for playing podcasts. For information on how these platforms retain data please see their respective privacy policies.	Subject to regular review.	Privacy and Electronic Communications Regulations 2003 Removed when no longer relevant otherwise retained for legitimate interest (subject to individual data subjects' rights).	Destroy
	Web articles	Subject to regular review.	Removed when no longer relevant otherwise retained for legitimate interest	Destroy

			(subject to individual data subjects' rights).	
	Cookies, IP addresses, metrics data and other online identifiers	For information on how third-party social media and statistical providers retain data on our website visitors and details on types of cookies and how long they are retained for, please refer to their respective Cookies Privacy Policies	Good practice/Privacy and Electronic Communications Regulations 2003	Destroy