POLICY HANDBOOK

Version 0.4
29/04/21

Table of Contents

Changes since last review

0.1	First created
0.2	First edit including comments from Steph
0.3	Added Data Retention Schedule
0.4	Added Finance Policies

1 Introduction

1.1 About the South Eastern Baptist Association

1.1.1 Vision Statement

As a regional Association we share the vision of Baptists Together, our national movement

'Growing healthy Churches in relationship for God's mission'

We are committed to intentionally developing a culture where we...

Seek to be a movement of spirit led communities:

As those who have encountered the living Christ, to intentionally seek his will and purpose for our local churches and every expression of our shared life (Gal. 5:22-25)

Feel like one team:

Celebrating diversity; valuing, respecting and trusting each other as we work together in partnerships – making sure everyone feels included and listened to (I Cor. 12:24b-27)

Embrace adventure:

Being serious about discipleship, willing to take risks, pioneer and move out of the comfort zone of familiar ways of doing things (Matt. 28:18-20)

Inspire others:

With a generosity of spirit, energise and motivate people to be all that God created them to be (Eph. 5:1-2)

Share a hunger for god's coming kingdom:

Nurturing a 'holy discontent' that arises from our desire to give practical expression to our vision of God's purpose for creation – confronting evil, injustice and hypocrisy and challenging worldly attitudes to power, wealth, status and security both within and beyond our Union. (Matt. 6:9-10)

1.1.2 Governance

The Trustees are responsible for the governance of the Association, supporting the Association through the provision of robust policies and ensuring that the association is compliant legally in all the areas of operation including HR, Finance, Risk management, Health & safety, Safeguarding, Administration, Logistics & Event management.

The Trustees are supported by the Leadership Team whose role is to inspire and envision the Association through a strategy that enlivens and equips Churches to make known the gospel of Jesus and his Kingdom.

1.2 Purpose of this Handbook

We believe that is important to recognising and use the variety of gifts and talents God has given His people to do His work and that each role in the organisation is of value and vital in making the Association function.

"Now there are different kinds of spiritual gifts, but the same spirit gives them. There are different ways of serving, but the same Lord is served. Working in all sorts of different ways and different people, it is the same God who is working in all of them." (I Corinthians 12:4-6)

We value and respect the talents that each member of staff brings to the Association and expect them to carry out their role effectively, efficiently, and with a right spirit of service so that the "body" — the Association as a whole — will function well. As a part of the Body of Christ, we share a common mission and pray that the Holy Spirit will enable us to share together in accomplishing that mission in the Spirit of Christ.

This Handbook has been put together to provide the policies and guidelines for all workers that are necessary to:

- achieve our aims and objectives and to allow us to operate in a way that respects our Christian ethos;
- provide appropriate levels of protection for potentially vulnerable children and adults who take part in our activities;
- meet legal requirements in relation to Employment, Health and Safety, Data Protection, etc.;
- safeguard our assets;
- ensure the efficient running of our activities.

All workers and Trustees must adhere to these policies and guidelines. Failure to do so could have implications for the Association. Violation of these policies could result in disciplinary action being taken against the individual concerned.

1.3 Glossary of Terms

The following terms used throughout this Handbook have specific meanings and are defined here to avoid confusion:

The Association – The South Eastern Baptist Association

Staff – Employees and Ministers

Employees – people who are paid to work for the Association and are not Ministers

Minister(s) – ordained members of staff

Volunteers – are those people who carry out a specific role within the Association without being paid

Workers – Staff and volunteers

Members – Baptist churches in the region in membership with the Baptist Union of Great Britain (BUGB)

2 Safeguarding

The Association, its leaders and trustees, have oversight of member churches within their region. Although they do not have direct responsibility for safeguarding practice within the churches, they have a support and challenge role, seeking to train, equip and support those with oversight of safeguarding. Every church is expected to have their own Safeguarding Policy and Procedures reflecting the needs of their own congregation. The Association strongly recommends that this is based on the BUGB Model Safeguarding Policy and Procedures.

2.1 Policy Objective

We are concerned with the welfare and wholeness of each individual, within God's purpose for everyone. We seek to safeguard all members of the Association including all ages. It is the responsibility of each one of us to prevent neglect and the physical, sexual, emotional, financial or spiritual abuse of children, young people and adults at risk. In fulfilling this objective, we will:

- Have an Association Safeguarding Officer with suitable training and experience to support churches with safeguarding matters
- Have a named safeguarding trustee responsible, along with the Association Safeguarding Contact, for promoting safeguarding practice across the life of the Association
- Promote Excellence in Safeguarding within the churches of the Association
- Offer support and advice to churches with safeguarding concerns or incidents
- Provide Excellence in Safeguarding training (Level 2 and 3) in line with the recommendations of the BUGB

2.2 Responsibilities

The Association recognises its responsibilities in safeguarding all children, young people and adults at risk associated with it, both directly and by supporting member churches.

We commit ourselves to the nurturing, protection and safeguarding of all those in our church communities, especially children, young people and adults at risk. In pursuit of this we commit ourselves to this policy and the development of sound procedures to implement our policy well.

2.3 Prevention and Reporting of Abuse

It is the duty of all workers to help prevent the abuse of children, young people and adults at risk and to respond to concerns about the well-being of those within our churches. Any abuse disclosed, discovered or suspected will be reported in accordance with our procedures. We will also support our churches to enable them to respond to concerns about the well-being of children, young people and adults at risk in line with our procedures.

2.4 Safe Recruitment, Support and Supervision of workers

The Association will exercise proper care in the selection and appointment of all workers, particularly those in a position of trust or working directly with children, young people or adults at risk. All workers will be provided with appropriate training, support and supervision to promote the safeguarding of children, young people and adults at risk.

2.5 Supporting Churches

The Association has a named person responsible for supporting churches managing safeguarding concerns (the Safeguarding Officer). They have completed Level 2 and 3 in Excellence in Safeguarding and understand the procedures for escalating safeguarding concerns. Where they are unsure about the best course of action they will

work with the National Safeguarding Team to ensure that the situation is managed well and those at risk are properly safeguarded.

2.6 Promote Best Safeguarding Practice

All workers are responsible for promoting best safeguarding practice amongst the churches they support. This includes seeking support from the Safeguarding Officer when necessary and following the advice that has been given.

2.7 Provide Training

The Association will facilitate safeguarding training for churches in our area using the Baptist Union Level 2 and 3 Excellence in Safeguarding material. We will ensure that we have knowledgeable and experienced trainers to facilitate the course who have completed the BUGB Train the Trainer course for each level. The Association will ensure that Level 2 and 3 safeguarding training is available to churches throughout the Region and widely promoted by all regional team members.

2.8 Working with national and statutory bodies

To ensure that children, young people and adults at risk within our churches are properly safeguarded, we will work closely with the BUGB National Safeguarding Team, statutory authorities, other denominations and uniformed organisations, sharing information where necessary.

Part of this commitment to working together to safeguard children, young people and adults at risk will include the Safeguarding Officer participating in the work of the National Safeguarding Contacts Group, which serves as a coordinating body for improvements in safeguarding policy and practice.

2.9 DBS Checks

The Association will initiate all DBS checks for Accredited Ministers and Regionally Recognised Ministers / Pastors using the Baptist Union account with DDC. Any blemished disclosures will be assessed by the National Safeguarding Team and recommendations will be passed to the Ministries Team in relation to BU Accredited Ministers and Nationally Recognised leaders. When the disclosure relates to a Regionally Recognised Minister the outcome of the risk assessment will be shared with the Safeguarding Office in the first instance.

DBS checks for Unaccredited Ministers are the responsibility of the local church. The Association has no legal right to know the information included in the check. However, the Association will request from the church the date and number of the DBS check and this will be recorded on the ThankQ database. This ensures consistency with the recording of information about ministers regardless of their accreditation status.

When an Unaccredited Minister has a blemished disclosure, the National Safeguarding Team will share any recommendations from the risk assessment directly with the church in the first instance. If they consider that the church needs support in implementing the recommendations from the risk assessment, then the Association will be advised of the situation.

2.10 Training

The Association will provide a timetable for safeguarding training throughout the region, using the BUGB Excellence in Safeguarding Level 2 and 3 material, and will promote the courses to churches in their area.

The Association will work with the National Safeguarding Team to identify and train specialist Excellence in Safeguarding trainers with a high standard of safeguarding knowledge and experience.

All Association trustees, regional ministers, youth and children's specialists and other pastoral staff will complete Excellence in Safeguarding Level 2 and 3 and work in accordance with the principles and teaching they have received through the courses.

2.11 Supporting and equipping Designated Persons for Safeguarding (DPS) withing member churches

It is the responsibility of each church to appoint at least one Designated Person for Safeguarding for their church. The Association will seek to offer specific support to the Designated Person for Safeguarding, particularly when safeguarding concerns arise. Where a church does not yet have anyone in this role, the Safeguarding Officer will work with the leadership of the church to help them to identify, train and support someone to take on this role.

The Association will provide opportunities for DPSs to access peer support. and, through the National Safeguarding Contacts Group, work with the National Safeguarding Team to identify additional online and written resources for people taking on this role.

2.12 Policy Review

These Safeguarding Policy and Procedures will be agreed by the Association Trustees and distributed amongst all members of the Association staff team. It will be reviewed on a 3-yearly basis.

3 Employment Policies

3.1 Equal Opportunities

The Association is committed to the promotion of equality of opportunity in all fields of its activity in conformity with this Policy Statement.

3.1.1 Definitions

- **'Protected Characteristic'** refers to gender, sexual orientation, colour, race, nationality or ethnic or national origins, marriage and civil partnership, pregnancy and maternity, disability, age, gender reassignment or religion or belief.
- **'Direct Discrimination'** is where a person is treated less favourably than others are, or would be, for a reason related to one or more of the 'Protected Characteristics'.
- **'Indirect Discrimination'** occurs where an individual is subject to a provision, criterion or practice which one protected group finds more difficult to comply with than another (even though the provision is neutral)

3.1.2 Policy Statement

The Association is an equal opportunities employer and will seek to ensure that:

- every applicant for a job and every employee has the right not be treated less favourably as a result of one or more Protected Characteristics except in relation to religious belief, where being a Christian or complying with a requirement related to religious belief, is an occupational requirement having regard to the ethos of the Association and the nature of the employment or the context in which it is carried out;
- persons already employed will be made aware of the provisions of this policy;
- the application of any recruitment, training and promotion policies will be solely on the basis of job requirements and the individual's ability and fitness for that work;
- all persons responsible for the selection, management and promotion of employees will be given information and/or training to enable them to minimise the risk of discrimination;
- appropriate training will be provided to enable employees to perform their jobs effectively and uphold the commitment to equality of opportunity;
- encouragement is given to all employees to take advantage of opportunities for training;
- any age limits imposed for entry to training will be objectively justified as a proportionate means of achieving a legitimate aim and will not unnecessarily exclude certain groups of employees;
- recruitment, literature and advertisements will not imply that there is a preference for one group of applicants as against another unless there is an occupational requirement which will be clearly stated and the application of that requirement is a proportionate means of achieving a legitimate aim;
- applicants for posts will be given clear, accurate and sufficient information through advertisement, job descriptions and interviews, to enable them to assess their own suitability for a post;
- the requirements of job applicants and existing members of staff who have or have had a disability will be reviewed to ensure that reasonable adjustments are made to enable them to enter into or remain in employment with the Association; promotion opportunities, benefits and facilities of employment will not be unreasonably limited and every reasonable effort will be made to ensure that disabled staff participate fully in the workplace;
- employment policies and procedures will be kept under review, in appropriate cases by formal monitoring routines, to ensure that they do not operate against the Association's Policy Statement;
- where it appears that the Association's Policy Statement is not being observed, the circumstances will be investigated to see if there are any policies or criteria which exclude or discourage employees and, if so, whether these policies and criteria are justifiable;

- appropriate action will be taken where necessary to redress the effects of any action, policy or criteria which are found to have unjustifiably limited the observance of the Association's Policy Statement;
- particular care will be taken to deal with any complaints of unlawful discrimination and harassment on the grounds of a Protected Characteristic;
- a criminal record is not in itself a bar to being appointed to any post. only relevant offences will be taken into account when appointing to a post where a DBS check is required.

3.2 Working with Ex-Offenders

As an organisation using the Disclosure and Barring Service (DBS) to assess applicants' suitability for positions of trust, the Association undertakes to treat all applicants for positions fairly. It undertakes not to discriminate unfairly against any subject of a Disclosure on the basis of conviction or other information received.

We welcome people to serve the Association on the basis of the right mix of talent, skills, character, potential and call of God, including those with criminal records.

Only where an applicant is applying for a post that requires an enhanced or standard DBS check will they be required to provide one as part of the application process.

A criminal record will not necessarily be a bar to a person serving with children and young people or vulnerable adults. This will depend on the nature of the position and the circumstances and background of the offences.

In order to protect the confidentiality of those with criminal records we will access Disclosures through Due Diligence Checks.

We will invite the Baptist Union's National Safeguarding Officer to advise us in the appointment process when necessary, and we agree to act on their advice for the protection of children and young people and adults at risk.

3.3 On-going Management and Development

3.3.1 Terms and Conditions of Service

The Association will treat all workers equally and create a working environment which respects their diverse backgrounds and beliefs. Terms and conditions of service for employees will comply with anti-discrimination legislation. This includes the provision of benefits such as flexible working hours, maternity, parental and other leave arrangements, performance appraisal systems and dress code.

3.3.2 Induction

When a new Employee joins the Association he or she will be welcomed by their line manager or another member of staff who has been given this responsibility and taken through the appropriate Induction Programme (according to the job role they will undertake) and will need to review the Policy Handbook. The briefing will also include details of the sickness, expenses, leave, hours of attendance, security arrangements and training.

The induction procedure will take place within two months of the individual joining the Association (unless justifiable reasons have been recorded). A record confirming the content and the date of the individual's induction will be kept on the individual's personnel file.

3.3.3 Support and Supervision

Where appropriate, Employees will have regular support and supervision meetings with their line manager. The purpose of support and supervision meetings is to enable both the Employee and their manager to discuss and progress work-related matters and to resolve any issues that may have occurred.

3.3.3.1 Appraisals for all staff

All staff will receive regular annual appraisals undertaken by an appropriate manager or fellow minister. The aim of appraisals is to discuss with individual members of staff the effectiveness of their work. They should involve objective setting and be tailored to the skills of the individual. Appraisals are also used to record training and development needs. Summaries of the actions proposed as a result of these discussions are to be recorded for future reference.

The appraisal procedure is not to be used for disciplinary purposes, however where there are areas for development, these should be identified and remedies worked out. It is very important during these discussions that the member of staff is able to put across their point of view and express any differences of opinion they may have. It must be stressed however that actual or perceived difficulties should be aired as soon as possible and never wait to be raised during a performance review.

3.3.3.2 Managing volunteer performance

The Association aims to ensure that all its volunteers are adequately supervised and supported to work to the performance and behavioural standards required. The Association is committed to addressing any issues in performance, behaviour or attitude via support and supervision. The management of volunteers within the Association will be fair, transparent, objective and respectful.

Although formal appraisals will not be carried out, reviews may take place from time to time with volunteers to ensure that any issues are being raised and addressed and also to solicit their input on any areas for improvement in the running of the Association.

3.3.4 Performance Management Process

Should any problems arise with employees' performance, they will be dealt with under the process outlined below and the employee will be made aware in writing of the particular issue and of each stage of the process, what it will entail and who will be involved. In the case of volunteers this is not a disciplinary process but should an employee be believed to have acted in a manner that has affected or could seriously affect the Association or its activities, the process outlined below will be followed.

An employee can be accompanied to any meeting by someone from the Association (either another employee or volunteer) at any stage of the process, but their role will be as a supporter, not an advocate.

Throughout the performance management process, details of the issue will only be shared with the relevant people in the Association. This will include the person to whom the employee reports and may also include a limited number of Trustees. At no time will details be shared more widely within the Association. A number of Trustees will need to remain independent in case the employee wishes to raise a complaint at a later stage.

Throughout the process, the employee will be given reasonable notice of any meetings and clear information about what is to be discussed and will be able to put over their point of view. Minutes of each meeting shall be taken and agreed by both parties.

At the start of each step, the Company Secretary should review the situation and confirm that the employee has been dealt with properly and fairly so far.

3.3.4.1 Informal Reviews

It is hoped that perceived problems will be picked up during regular support and supervision meetings with employees. These meetings will be undertaken by the person to whom the employee reports. Many 'problems' are simply due to a lack of skills or knowledge, or a lack of support, inappropriate roles etc., and will be relatively easy to put right. Consideration will be given to any special requirements the employee may have and reasonable adjustments made.

A written record of any supervision and support meetings will be kept. Action agreed by both parties will be followed up within an agreed and appropriate timescale.

Sometimes, an employee may be unaware that they are doing something wrong. The Association will advise the employee of what is expected of them and be given feedback on their progress.

Informal methods of resolution may include coaching, shadowing or training, other forms of learning, one-to-one support, or even a change of role. The Association will consider other suitable roles for its employees where appropriate.

3.3.4.2 Formal Reviews

Where informal measures do not resolve the problem, the employee will be invited to a formal meeting with the person to whom they report and the Company Secretary. The aim of the meeting is to agree an action plan to remedy the problem and improve performance or behaviour, with appropriate timescales. The employee will be reminded what the problem is and what standards they need to achieve. The employee will be able to present their point of view and explain the situation from their perspective.

If the issue is not resolved within the agreed timescale, another meeting involving the employee, the person to whom the employee reports and the Company Secretary will be called at reasonable notice (not less than one week). This meeting may result in an employee having their contract of employment terminated or a volunteer being asked to leave.

3.3.5 Continuing Ministerial Development

We recognise that no minister can learn at college all they need to learn and no minister can operate in isolation from the support, friendship and advice of others in ministry. We believe that a healthy approach to ministry involves a commitment to both ongoing learning and accountability and that this benefits the minister themselves, their families and the Association.

To this end we will give ministers time and financial support for their development and require them to engage with the Baptists Together Continuing Ministerial Development programme.

3.4 Disciplinary Action

This procedure is designed to help and encourage all employees of the Association to achieve and maintain standards of conduct, attendance and performance in their ministry/work. The aim is to ensure consistent and fair treatment for all. This procedure applies to all employees of the Association and will normally be followed where a breach of discipline occurs but the procedure is not contractually binding upon the Association and is for guidance only.

Where possible, matters will be dealt with informally, but where the matter is more serious either a capability hearing or a disciplinary hearing will be held (see Sections 2.1 and 2.2).

3.4.1 Principles

- No disciplinary action will be taken against an employee until the case has been fully investigated.
- No employee will be dismissed for a first breach of discipline except in the case of gross misconduct for which an individual may be dismissed without notice or payment in lieu of notice.
- An employee will have the right to appeal against any disciplinary penalty imposed.
- The procedure may be implemented at any stage if the employee's alleged misconduct warrants such action.

3.4.2 Concurrent Procedures

In the event that an employee submits a grievance during a disciplinary procedure, the Association may at its discretion, decide whether to suspend the disciplinary procedure in order to fully consider the grievance, or to deal with both procedures concurrently, where the issues are related.

3.4.2.1 Establishing the facts

The Association will investigate, without delay, any allegation or indication of poor performance or misconduct. In some cases, this will require an investigatory meeting, held by a senior Association representative, to establish the true facts in the matter.

The Association may consider it necessary to suspend the employee on full pay pending investigation.

3.4.2.2 Suspension

The Association may at any time suspend the employee for a reasonable period of time, during any period in which the Association is carrying out a disciplinary investigation into any alleged acts or defaults of the employee. During any period of suspension, the employee shall continue to receive their salary and contractual benefit. This is not disciplinary action, but a neutral act pending the outcome of the investigation.

3.4.2.3 Informing the employee

If, following the investigation, either misconduct or unsatisfactory performance is confirmed and it is felt that there is a disciplinary case to answer, the employee will be asked to attend a formal meeting and the employee will be notified in writing that disciplinary action may follow. This notification will contain sufficient information about the alleged misconduct or poor performance to allow the employee to prepare a response for any disciplinary hearing. It will also include any evidence gathered during the investigation, which supports the decision to take disciplinary action.

The employee will also be informed of the time, date and venue of the disciplinary hearing, and advised of the employee's right to be accompanied by a colleague or trade union representative.

3.4.2.4 Disabilities

Consideration should always be given to whether poor performance may be related to a disability and, if so, whether there are reasonable adjustments that could be made to the employee's working arrangements, including changing his/her duties or providing additional equipment or training. The Association may also consider making adjustments to this procedure in appropriate cases.

If the employee wishes to discuss this or inform the Association of any medical condition which they consider relevant, they should contact their Line Manager or the Company Secretary.

3.4.2.5 Confidentiality

The Association's aim is to deal with performance matters sensitively and with due respect for the privacy of any individuals involved. All employees must treat as confidential any information communicated to them in connection with a matter, which is subject to this disciplinary procedure.

The employee and anyone who accompanies them (including witnesses) must not make electronic recordings of any meetings or hearings conducted under this procedure.

The employee will normally be told the names of any witnesses whose evidence is relevant to their disciplinary hearing, unless the Association believes that a witness's identity should remain confidential.

3.4.2.6 Notification of a hearing

If the Association considers that there are grounds for taking formal action over alleged poor performance, the employee will be required to attend a capability hearing. The Association will notify the employee in writing of its concerns over the individual's performance, the reasons for those concerns, and the likely outcome if it decides after the hearing that the employee's performance has been unsatisfactory. The Association will also include the following where appropriate:

- a summary of relevant information gathered as part of any investigation;
- a copy of any relevant documents which will be used at the capability hearing;

- a copy of any relevant witness statements, except where a witness's identity is to be kept confidential, in which case the Association will give the employee as much information as possible while maintaining confidentiality.

The Association will give the employee written notice of the date, time and place of the capability hearing. The hearing will be held as soon as reasonably practicable, but the employee will be given a reasonable amount of time, to prepare their case based on the information which the Association gives them.

3.4.2.7 Right to be accompanied at hearings

The employee may take a companion to any capability hearing or appeal hearing under this procedure. The companion may be either a trade union official or a fellow employee. The employee must tell the manager conducting the hearing who their chosen companion is, in good time before the hearing.

Employees are allowed reasonable time off from duties without loss of pay to act as a companion. There is no duty on employees to act as a companion if they do not wish to do so.

If the chosen companion will not be available at the time proposed for the hearing the employee may request that the hearing be postponed to a day not more than five working days after the day proposed by the Association. If the time proposed is reasonable, and the employee representative is able to attend, the hearing will be postponed until that time.

Whilst the companion may address the hearing and confer with the individual during the hearing, they do not have the right to answer questions on the part of the individual.

If the employee's choice of companion is unreasonable the Association may require them to choose someone else, examples include:

- if, in the Association's opinion, the employee's companion may have a conflict of interest which may prejudice the hearing;
- if the employee's companion works at another site and someone reasonably suitable is available at the site at which they work;
- if the employee's companion is unavailable at the time a hearing is scheduled and will not be available for more than five working days.

The Association may, at its discretion, allow the employee to take a companion who is not an employee or union official (for example, a member of their family) where this will help overcome a particular difficulty caused by a disability, or where the employee has difficulty understanding English.

3.5 Grievance

The Association realises the importance of good working relationships. For this reason, it aims to establish an atmosphere in which problems can be discussed and resolved by encouraging open communication. The Association also believes that it is in everyone's best interest to ensure that employee's grievances are dealt with quickly and fairly and that a grievance procedure enables individuals to raise issues with management that affect them in the workplace.

The Association will try to resolve, as quickly as possible, any grievance which an employee may have about their work or about actions of the Association or their colleagues. The procedure is non-contractual but applies to all employees who should familiarise themselves with its provisions.

Where Ministers have a grievance the Association will use the Baptist Union procedure entitled "Grievance Procedures for Baptist Ministers in Pastoral Charge", found at The Baptist Union of Great Britain : Grievance Procedures for Baptist Ministers in Pastoral Charge.

3.5.1 Concurrent Procedures

In the event that an employee submits a grievance during a disciplinary procedure, the Association may at its discretion, decide whether to suspend the disciplinary procedure in order to fully consider the grievance, or to deal with both procedures concurrently, where the issues are related

3.5.2 Mediation

In appropriate circumstances, the Association may suggest mediation as a means of addressing a grievance. Mediation may take the form of a neutral mediator, assisting parties to reach an amicable outcome to a grievance. Mediation will usually take the form of an open session between all affected parties and the mediator at which each party will state its case, followed by a series of meetings between each party and the mediator.

3.6 Flexible Working

The Association will consider requests from employees for flexible working, which could include part-time work, working from home or job-sharing. To be eligible an employee must have been continuously employed for 26 weeks at the point of making the request.

The employee must specify in a written application the change in their contract that they seek and the date on which they would like the change to be implemented. The employee must also specify the effect that they think the change will have on the Association and suggest how these effects could be dealt with. Each employee may only make one application per year.

The Association will aim to handle the request as quickly as possible and will in any event deal with the whole process, including any appeal, within a three-month period. Once a written request has been received, the Association will arrange to meet with the employee, and the employee has the right to be accompanied. The application will be considered carefully but may be refused due to the burden of additional costs, a detrimental effect on the ability to meet 'customer demand', the inability to reorganise work among existing staff and a detrimental impact on quality or performance.

The Association will give their decision to the employee in writing. Where the decision is to refuse the application, we will state which of the grounds for refusal are considered to apply, explain why those grounds apply in relation to the application, and advise the employee of their right to appeal. An employee does have the right to appeal against the employer's decision.

If a flexible pattern of working is agreed this will be confirmed formally. Once a flexible arrangement is agreed, the employee does not have a right to revert to the previous arrangement. However, a trial period will normally be arranged in which the new arrangements can be tested, providing an option to return to the previous way of working.

3.7 Maternity Leave

Statutory Maternity Leave is 52 weeks and is made up of:

- Ordinary Maternity Leave - first 26 weeks
- Additional Maternity Leave - last 26 weeks

A member of staff is not required to take 52 weeks but must take at least 2 weeks' leave after a baby is born.

Usually, the earliest date Maternity leave can start is 11 weeks before the expected week of childbirth and will automatically start:

- the day after the birth if the baby is early
- automatically if the member of staff is off work for a pregnancy-related illness in the 4 weeks before the week that the baby is due

Pregnant members of staff will be given paid time off work to attend appointments for antenatal care.

Statutory maternity pay will be paid at the rate of 90% of the employee's normal weekly earnings for the first six weeks and at a flat rate up to 33 further weeks.

In order to claim maternity pay a member of staff must have:

- 26 weeks' continuous service up to and including the 15th week before the expected week of childbirth;
- Become pregnant and have reached or given birth before reaching the start of the 11th week before the expected week of childbirth;
- Have started a period of maternity leave
- Average weekly earnings for the 8 weeks up to and including the 15th week before the expected week of childbirth equal to at least the lower earnings limit for the payment of primary class one national insurance contributions.
- Given 28 days' notice to the Association of the date when she expects liability for statutory maternity pay to begin or if 28 days' notice was not reasonably practicable, such lesser notice as was practicable;
- Produced medical evidence of the pregnancy and of the expected week of childbirth.

3.8 Paternity Leave

Fathers who have completed 26 weeks' continuous service ending with the week preceding the fourteenth week before the expected week of childbirth may take two weeks' paternity leave within 56 days of a child's birth and will be paid statutory paternity pay or 90% of the employee's normal weekly earnings if that is lower.

Fathers must give the Association 28 days' notice of their intention to take paternity leave.

3.9 Shared Parental Leave

Staff may be entitled to Shared Parental Leave (SPL) and Statutory Shared Parental Pay (ShPP) where they are the parents of children born or adopted after 5 April 2015.

Staff can start SPL if they're eligible and they or their partner end their maternity or adoption leave or pay early. The remaining leave will be available as SPL. The remaining pay may be available as ShPP. (ShPP is paid at the same rate as SMP). Sometimes only one parent in a couple will be eligible to get Shared Parental Leave (SPL) and Statutory Shared Parental Pay (ShPP). This means that they can't share the leave.

Eligible staff can take SPL in up to 3 separate blocks. They can also share the leave with their partner if they're also eligible. Parents can choose how much of the SPL each of them will take.

For example, a mother could end her maternity leave after 12 weeks, leaving 40 weeks (of the total 52 week entitlement) available for SPL. If both the mother and her partner are eligible, they can share the 40 weeks. They can take the leave at the same time or separately.

SPL and ShPP must be taken between the baby's birth and first birthday (or within 1 year of adoption).

To qualify for SPL, the child's mother (or adoptive parent) must be eligible for either maternity leave or pay, Maternity Allowance or adoption leave or pay

The member of staff must also:

- have worked for the Association continuously for at least 26 weeks by the end of the 15th week before the due date (or date they are matched with their adopted child)
- still be employed by the Association while they take SPL
- give the Association the correct notice including a declaration that their partner meets the employment and income requirements which allow the employee to get SPL

3.10 Adoptive Parents

Parents who adopt a child will be entitled to one year's adoption leave commencing either on the date on which the child is placed for adoption or on a date no more than 14 days before the expected date of placement.

To be eligible for adoption leave, a parent must have completed 26 weeks' service by the time they are matched with a child.

Where a couple jointly adopt, only one of them will be entitled to take adoption leave but the other parent will be entitled to take statutory paternity leave.

The member of staff must give the Association notice of their intention to take adoption leave within seven days of being notified of having been matched with a child.

Statutory adoption pay will be paid for 39 weeks at the same flat rate as statutory maternity pay.

3.11 Parental Leave

Staff with at least one year's continuous service are entitled to take unpaid parental (called 'Ordinary Parental Leave) for the purpose of caring for the child if they are the parent of a child who is under 18 years old, or if they have adopted a child under the age of 18. Staff may take a maximum of 18 weeks' unpaid parental leave. The member of staff's right to take leave lasts until a child's 18th birthday. Ordinary parental leave is available for each child. If an employee has, for example, two children under the age of 18, he or she may take 18 weeks' unpaid parental leave in respect of each of those children.

Leave can be taken in blocks or multiples of one week (unless the child has a disability in which case leave may be taken in blocks of one day) and employees may be required to give notice of their intention to take leave. Staff may only take four weeks' leave in any twelve-month period and leave may be postponed by the Association for up to six months where the work of the Association would be unduly disrupted. However, leave cannot be postponed when the member of staff gives notice to take it immediately after the time the child is born or is placed with the family for adoption.

3.12 Time Off for Dependants

Staff are entitled to a reasonable amount of unpaid time off in order to take action which is necessary:

a) to provide assistance on an occasion when a dependant falls ill, gives birth, is injured or assaulted;
b) to make arrangements for the provision of care for a dependant who is ill or injured;
c) in consequence of the death of a dependant;
d) because of the unexpected disruption or termination of arrangements for the care of the dependant;
e) to deal with an incident which involves a child of the employee and which occurs unexpectedly in a period during which no educational establishment which the child attends is responsible for him.

This right does not arise unless the member of staff informs the Association of the reason for their absence as soon as reasonably practicable and tells the Association how long they expect to be absent.

For these purposes, a dependant means a spouse, a child, a parent, or a person who lives in the same household as the employee, otherwise than by being his employee, tenant, lodger or boarder.

For the purposes of (a) and (b) above, dependant also includes any person who reasonably relies on the member of staff for assistance on an occasion when the person falls ill or is injured or assaulted or to make arrangements for the provision of care in the event of illness or injury.

For the purpose of (b) above, dependent includes any person who reasonably relies on the employee to make arrangements for the provision of care.

3.13 Retirement

3.13.1 Retirement Age

The Association does not have a fixed retirement age. This position will be reviewed periodically with a view to introducing a fixed retirement age if this would reflect the needs of the Association and providing the change can be objectively justified.

Staff are free to retire when they wish to do so and will not be pressurised into retiring because they have reached, or are approaching, a certain age.

3.13.2 Discussing Future Plans

The Association encourages all staff to discuss their short, medium and long-term plans as the need arises. We may also want to initiate these discussions with staff in order to plan for the needs of the Association.

If a workplace discussion does take place, we will aim to make it as informal as possible. We will not assume that staff want to retire just because they are approaching a certain age and will not make discriminatory comments, suggesting that they should move on due to age.

We will not make generalised assumptions that performance will decline with age, whether due to competence or health issues. If there are problems with performance or ill-health, these will be dealt with in the usual way, through the Capability procedure or Sickness Absence procedure.

3.13.3 Giving notice of retirement

Once a member of staff has decided to retire, they should give at a minimum the notice they are obliged to under their contract or terms of employment.

3.14 Staff Pensions

All staff who are aged between 22 and State Pension Age and who earn over the automatic enrolment earnings trigger (as defined annually by the Government) will be offered membership of the Baptist Pension Scheme. There are two sections which the member of staff can choose between (more details will be provided at the time of making a choice).

- **Ministers and staff section,** which requires higher levels of contribution and offers death and income protection benefits.
- **Basic section,** which has lower levels of contribution but does not provide income protection benefits.

A member of staff choosing not to join either of these sections, will be auto-enrolled into the National Employment Savings Trust - Government Pension scheme (NEST). Further details will be provided at the time the member of staff is making their choice. The member of staff will have the option to opt out from this scheme, in which case they will be automatically re-enrolled every 3 years (again with an option to opt out). If they remain in the scheme the contributions will be in line with the requirements of the scheme.

Staff aged between 22 and State Pension Age who earn above the lower level of qualifying earnings as set by the Government but below the automatic enrolment earnings trigger, will be admitted to the scheme of their choice (as described above) on request, but this will not be automatically offered and auto-enrolment will not apply.

Other member of staff (i.e. those under age 22, aged over State Pension Age or earning below the lower level of qualifying earnings) will not be entitled to a pension provided by the Association.

4 Finance

4.1 Finance and General Purposes Committee

The SEBA Trustees have established a Finance and General Purposes Committee in order to address a number of finance related issues and report back to the Trustees.

4.1.1 Membership

The committee will be chaired by the Association Treasurer and include

- The Operations Manager
- At least one Regional Minister
- Up to three people appointed by the Executive

A quorum shall be not less than half those eligible to attend.

4.1.2 Responsibilities

- To prepare an annual budget for presentation to the Trustees in October.
- To monitor income and expenditure in relation to the budget.
- To agree an annual target for Home Mission giving with the Trustees and Leadership Team and to monitor the giving receipts.
- To set an annual budget for Home Mission grants.
- To review grant proposals from the Leadership to monitor compliance with agreed criteria
- To monitor income and expenditure on the properties for which the Association is responsible.
- To consider any other financial matters, as applicable.

4.2 Reserves

4.2.1 Background

Reserves are required to meet future shortfalls in income or unexpected expenses.

The Association is reliant for our income on a Home Mission grant from the Baptist Union, supplemented by the rental income form the properties we own and donations. If income were to drop suddenly, then reserves would be needed to cover the income lost less whatever savings could quickly be made from expenditure. If the fall is a longer-term loss of income, more significant cuts in expenditure would need to be made. Reserves would be needed to tide us over the period in which these cuts could be put into place.

4.2.2 Level of Reserves Required

We will hold in free reserves (unrestricted reserves that are readily accessible) the greater of the following two calculations:

1. One month's budgeted expenditure.
2. The difference between the budgeted levels of expenditure based on nine months of any costs associated with employees/ministers, three months' worth of all other budgeted items, and six months of our budgeted income.

A minimum of one month's budgeted income should enable us to meet any short-term volatility in income. We are committed to certain items of expenditure, even if our income were to fall dramatically. For example, if we were considering reducing staffing levels, some future cost would still be incurred (e.g. redundancy costs, pay during the

notice period). Ensuring reserves are at least equal to the second calculation will enable us to meet expenses we are committed to in the event of a longer-term fall in income.

The amount will be calculated each year when the budget is set for the following year.

4.2.3 Corrective Action

If our reserve levels fall below the required amount, we will consider deferring/ceasing certain items of expenditure.

4.2.4 Monitoring and reviewing the policy.

The deacons receive monthly reports of income and expenditure, and these are monitored to ensure that our reserve level is adequate.

The policy will be reviewed each year together with the proposed budget.

4.3 Spending limits

The following levels of expenditure can be approved by the roles shown:

- Over £20 and up to £200 - Team Leader or Operations Manager.
- Over £200 and up to £500 - Treasurer.
- Over £500 and up to £1,000 – Finance Committee
- Over £1,000 – Trustee Board

The exception is an emergency repair to any Association property or equipment that cannot wait and can be approved by the Treasurer, but should be presented to the next Finance Committee or Trustee meeting.

Expenses approved in the church budget (e.g. insurance) will not require further church meeting approval.

Three quotations should be obtained for any new item of work or equipment to be purchased where the expenditure is over £500. The Finance Committee will agree which provider to use (this will not necessarily be the cheapest in all cases). In some instances, work may be agreed with only one quote:

- Where there is an existing relationship with a local provider and no concerns have been raised about previous work.
- An emergency repair.
- Work where only one or two providers are willing and able to provide a quotation.

4.4 Authorisation

The Treasurer, Operations Manager, Bookkeeper and Administrator will all have access to online banking, but the Administrator will not be able to authorise transactions. The Treasurer, Operations Manager, Bookkeeper and two further Trustees will be designated as authorised signatories on the Association bank accounts. Other accounts will be controlled by the Treasurer and Operations Manager.

All cheques, direct debits and standing orders will require two signatures.

All on-line payments, except for transfers between different Association accounts, will require to be set up be one signatory and authorised by another. Transfers between accounts can be done by a single user.

Any cheques or online payments to an authorised signatory or a family member of an authorised signatory should be signed/approved by two other authorised signatories.

4.5 Payment of expenses

Where a member of staff needs to incur travel or other expenses in the performance of their duties, these can be claimed back using the form and at the rates shown in Appendix 3. To claim the mileage allowance for the use of a private vehicle on SEBA business, the member of staff must provide evidence that the vehicle insurance includes cover for business use.

4.5.1 Hotel or B&B accommodation

Where a member of staff is required to stay away from home overnight in the performance of their duties, SEBA will meet the cost of overnight room and breakfast, provided prior approval has been obtained from the Operations Manager, Team Leader or Treasurer.

4.5.2 Travel arrangements

When travelling with colleagues, we expect staff to discuss the most cost effective way for everyone to travel to a meeting. This may involve one or more people travelling to other locations first so that the whole group can travel in one car to reduce overall expenses. However, we recognise that time, distance and practical arrangements will need to be taken into account.

4.5.3 Travelling by air

In exceptional circumstances staff may need to book flights to attend conferences or events. Before making any flight arrangements mileage prior approval must be obtained from the Operations Manager, Team Leader or Treasurer.

5 Health and Safety

5.1 General statement of policy

The Association recognises and accepts its responsibilities as an employer for providing so far as is reasonably practicable, a safe and healthy environment on and within its own offices and storage facilities, and at outside association events, with a view to ensuring the health, safety and welfare of all its staff, visitors and contractors. It is our policy that all activities and work will be carried out in a safe manner, and our target is for zero accidents and zero work-related ill health to be achieved by applying good health and safety practices and complying with any relevant statutory provisions where they apply.

This policy is designed to meet our duty under Section 2(3) of the Health and Safety at Work etc. Act 1974.

The Trustees of the Association will ensure that adequate resources are made available to achieve this objective and any decisions made will have due regard for it. They will monitor the effectiveness of this policy and amend it where it is no longer valid.

The Operations Manager will have specific responsibility for this policy and its implementation and to keep health and safety matters under review at appropriate intervals.

It is the duty of each Worker to exercise personal responsibility for their own safety and that of others and this policy will be brought to their attention. We will try to ensure that everyone involved with the Association plays his or her part in its implementation.

5.2 Responsibilities

The Operations Manager will ensure that:

- the standards set out in this policy are implemented and maintained
- where necessary, specialist health and safety assistance is obtained
- any hazards reported to them are rectified immediately
- only competent persons carry out repairs, modifications, inspections and tests
- any accidents are investigated, recorded and reported if necessary
- relevant health and safety documents and records are retained
- they keep up to date on health and safety matters relevant to the Association
- set a personal example on matters of health and safety.

The Trustees will ensure that:

- all employees and volunteers are aware of their health and safety responsibilities
- adequate precautions are taken as set out in this policy and related risk assessments
- adequate information and training is provided for those that need it
- any hazards or complaints are investigated and dealt with as soon as possible
- where defects cannot be corrected immediately, interim steps are taken to prevent danger
- all accidents are reported in-line with the requirements of this policy
- advice is sought where clarification is necessary on the implementation of this policy
- set a personal example on matters of health and safety.

All workers have a responsibility to cooperate in the implementation of this policy and to take reasonable care of themselves and others while on Association business. They will ensure that they:

- read this policy and understand what is required of them

- complete their work taking any necessary precautions to protect themselves and others
- comply with any safety rules, operating instructions and other working procedures
- report any hazard, defect or damage, so that this might be dealt with
- warn any new employees or volunteers of known hazards
- attend any training required to enable them to carry out their duties safely
- do not undertake any repair or modification unless they are competent to do so
- report any accident
- do not misuse anything provided in the interests of health and safety.

5.3 Arrangements

This section sets out our general arrangements for managing health and safety and dealing with

specific risks.

5.3.1 General Arrangements

5.3.1.1 Competent Assistance

Where necessary, we will appoint someone who is competent to assist us in meeting our health and safety obligations.

5.3.1.2 Risk Assessment

We will complete risk assessments to identify what we need to do to comply with health and safety law. We will record our findings, implementing any necessary precautions. We will review and revise these where we suspect that they are no longer valid.

5.3.1.3 Information and Training

We will provide any necessary information and training for our employees and volunteers in a timely manner. We will keep a record of what is provided. We will also give relevant information to contractors and self-employed people who may need this to complete their work safely.

5.3.1.4 First Aid

We will ensure that adequate first aid facilities are available at all events including – as a minimum – a suitably stocked first aid box and a person who will take charge of the first aid arrangements. We will also provide relevant information for employees and volunteers.

5.3.1.5 Accident Reporting

We will keep an accident book and record details therein. We will report to the enforcing authority and keep records of certain accidents to workers and members of the public in accordance with the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations.

5.3.1.6 Monitoring

We will make periodic checks to ensure that our precautions remain effective and adequate. We will also ensure that any lifting, work or electrical equipment are inspected as necessary to ensure that they remain safe. We will keep records of the checks we make.

5.3.1.7 Contractors

If we employ contractors, we will make sure that they have their own health and safety policy and Public and Employers Liability Insurance by asking to see copies of the relevant documents.

5.3.2 Specific Arrangements

5.3.2.1 Display Screen Equipment

Where workers regularly use computers daily, for continuous periods of an hour or more, we will analyse workstations to identify precautions, implementing these as necessary. We will also provide information, training, eye/eyesight tests (on request) and special spectacles if needed.

5.3.2.2 Driving on Association business

We recognise that driving is an integral part of the working day for some of our team, and we will make sure that all those driving on association business are safe to do so.

To this end, we will ask all staff to provide a copy of their driving licence when they join the association and to let us know if there are any endorsements to their driving licence or if they are disqualified from driving.

Staff will:

- be responsible for their own safety, for any passengers or loads carried in the vehicle and for ensuring that the vehicle is safe to use (including hired vehicles) including the use of seatbelts and the regular servicing of their vehicle;
- ensure that passengers are carried only in accordance with the vehicle manufacturer's design specification, with a seat for everyone and only one person per seat;
- on a long journey take regular breaks to help relax and reduce tiredness; and
- not stop on the hard shoulder of a motorway except in an emergency.

If any member of staff believes that they are driving excessive miles, or that they are unsafe to drive in particular circumstances (including changes in their health) they should speak to their manager immediately.

5.3.2.3 Electricity

We will ensure that any electrical system, fixed machine and portable appliance is maintained so as to prevent danger. Any defective equipment will not be used until it is repaired or replaced. We will keep records of the checks made where appropriate.

5.3.2.4 Events

Where we intend to hold large or unusual concerts, services and fundraising events, we will identify any additional precautions that are necessary and implement these.

5.3.2.5 Home Working

We will carry out an annual review of any risks that may be present in the Association properties. We will also ask any member of staff who works from home on a regular basis to complete a self-assessment form (see Appendix 4). These assessments will be reviewed by their manager who will take any necessary actions.

5.3.2.6 Manual Handling

We will avoid the need for lifting or carrying heavy objects as far as is possible. Where this is not practical, we will make use of lifting aids (such as trolleys) or other precautions including team lifting.

5.3.2.7 Preparation of Food

We will ensure that on those occasions when we prepare food, we use a clean and disinfected work surface, utensils and equipment. We will store food in such a way as to avoid contamination, provide hand-washing facilities and suitable arrangements for the disposal of waste.

5.3.2.8 Working at Height

Where possible, we will try and avoid the need for work at height. Where this is not practicable, we will ensure that any work is properly planned to identify suitable precautions. We will make sure that these are implemented, including the provision of any training and checks to ensure the safety of any equipment used.

5.3.2.9 Working Alone

We will identify circumstances where our employees and volunteers work alone and implement suitable precautions to ensure their safety.

6 Data Protection

6.1 Policy Statement

We are committed to protecting personal data and respecting the rights of individuals whose personal data we collect and use. We are registered as a data controller with the Information Commissioner's Office (ICO) with registration number Z2441527 and process the personal information of individuals in accordance with our constitution.

We process personal data to enable us to, among other purposes:

- Provide a voluntary service for the benefit 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;

Everyone has rights with regard to the way in which their personal data is handled. In line with our values and aims, we are committed to good practice in the handling of personal and confidential information and to ensuring that such information is stored securely and is processed in accordance with the law.

6.2 Purpose of this Policy

In the course of our work, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, contractors who provide us with technical services or payment services).

We process the personal information of individuals in both electronic and paper form and all this data is protected under data protection law. In some cases, it is sensitive information about individuals' religious or other beliefs, finances and personal circumstances. In addition, we hold lots of less sensitive information such as names and contact details, education and employment details, and visual images of individuals connected with member churches; current, past and prospective staff; volunteers; supporters; advisers; complainants and enquirers; representatives of other organisations; as well as business and other contacts such as suppliers. We may also receive other personal information from the above or other sources.

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.

We are aware that individuals can be harmed if their personal information is misused, is inaccurate, if it gets into the wrong hands as a result of poor security or if it is disclosed carelessly. We are committed to protecting personal data and information from unauthorised disclosure and ensuring its accuracy.

The purpose of this policy is to set out what measures we are committed to taking, as an organisation and as individual members of staff, to ensure we comply with the relevant legislation including:

- The Retained General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018 (DPA);
- The Privacy and Electronic Communications Regulations (PECR);
- The Computer Misuse Act 1990 (CMA);
- The common law duty of confidentiality;
- Any other laws and regulations relating to the protection of personal data.

Breaches of data security or confidentiality are serious incidents. If they occur they will be investigated fully and actively managed to ensure that any breach is as limited as possible. A breach of the UK GDPR, the DPA or other legislation may mean that we, and/or a member of our staff, are liable to prosecution or to regulatory action. We may also be required to report breaches to the Information Commissioner's Office (ICO) if a breach results in a risk to an individual, and to inform the data subject if the breach results in a high risk to any person.

6.3 Development of this Policy

This policy has been approved by the Board of Trustees which is responsible for ensuring that we comply with all our legal obligations. It sets out the legal rules which apply whenever we obtain, store or use personal data.

Our Data Protection Officer is responsible for ensuring compliance with data protection law, dealing with data security breaches and with the development of this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the Data Protection Officer at dataprotection@seba-baptist.org.uk. The Data Protection Officer will:

- Keep the content and effectiveness of this policy under review;
- Oversee compliance with the policy;
- Keep a record of all data security incidents or breaches and investigate in appropriate detail;
- Provide or arrange training and guidance for staff;
- Act as our nominated contact with the ICO.

References in this policy to the Data Protection Officer shall be construed as references to the Data Protection Officer or such other person as the Data Protection Officer may appoint to act on his or her behalf.

From time to time we may need to make changes to this policy or guidance in line with current operational practices and/or legislation.

Any questions, ideas or concerns about the operation of this policy or recommendations for additions or amendments should be referred to the Data Protection Officer.

6.4 Training and Guidance

We will provide general training at least annually for all staff to raise awareness and outline the law. We may also issue guidance or instructions from time to time. Managers must set aside time for their team to look together at the implications for their work.

6.5 Definitions of Data Protection terms

The UK GDPR (and this policy) applies

- to the processing of personal data wholly or partly by automated means and
- to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

The first part covers all data processing which involves the use of a computer ('processing' broadly covers all forms of handling of data, including storing and accessing it. The term is defined in more detail below).

The second part covers processing which does not involve a computer, of data which either forms part of a filing system, regardless of how well-structured it is, or which is collected in order to be added to a filing system at a later time (e.g. notes of a telephone conversation which are intended to be transferred to a file), even if the data is not actually added.

The following terms are used throughout this policy and bear their legal meaning as set out within the UK GDPR. The UK GDPR definitions are further explained below for the sake of clarity:

Data subjects include all living individuals about whom we hold or otherwise process personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects for whom we are likely to hold personal data include:

- Our employees;
- Individuals who are accredited or recognised for national Baptist ministry or who are working towards this;
- Consultants/individuals who are our contractors or employees working for them;
- Volunteers;
- Individuals in key roles in churches in membership, or linked, with us;
- Trustees;
- Complainants;
- Supporters;
- Enquirers;
- Advisers and representatives of other organisations.

Personal data means any information relating to a natural person who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons. In addition, personal data is limited to information about living individuals and does not cover deceased persons.

An 'identified' natural person is one who is identified from the data. An 'identifiable natural person' on the other hand is one who is not identified from the data itself but who can be identified, directly or indirectly, by reference to other data, such as an identification number, location data, an online identifier or to one or more factors specific to that person.

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if such decisions are taken alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process and this policy is intended to explain how we will comply with the UK GDPR.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that, as mentioned above, staff of data processors may also be data subjects).

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.

Special category personal data includes information about a person's:

- Racial or ethnic origin;
- Political opinions;
- Religious or similar (e.g. philosophical) beliefs;
- Trade union membership;
- Health (including physical and mental health, and the provision of health care services);
- Genetic data;

- Biometric data;
- Sexual life and sexual orientation.

Other than in the circumstances described below, information relating to criminal convictions and offences should not be processed unless the processing is authorised by law or is carried out under the control of official authority. This includes information about (i) allegations of criminal offences; (ii) proceedings in relation to criminal offences or alleged offences; and (iii) the disposal of criminal proceedings including sentencing. Special category personal data can only be processed under strict conditions, including the data subject's explicit consent (although other alternative conditions can apply in limited, very specific circumstances as described below).

The processing of special category personal data or personal data relating to criminal convictions and offences by accredited, nationally recognised and non-accredited ministers who are in active ministry in a Baptist church or who may return to active ministry, or by an individual in membership or in regular contact with a Baptist church or other member of the Union may, where strictly necessary, be carried out to safeguard against any risks posed to others under Article 6(1)(f) UK GDPR where the processing is necessary for the purposes of the legitimate interests of the Union, 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 convictions etc data ("criminal offence data") may also be processed by the Union 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.

6.6 Data protection principles

Anyone processing personal data must comply with the UK GDPR's Principles. These provide that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- processed for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purpose;
- accurate and, where necessary, up to date;
- not kept longer than necessary for the purpose, unless it is retained for public interest, scientific, historical research or statistical purposes and appropriate measures are taken to safeguard the rights of data subjects;
- processed in a manner which ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational means.

Personal data must also be processed in accordance with the rights of data subjects

Personal data cannot be transferred (or stored) outside the United Kingdom (UK) unless this is permitted by the UK GDPR (see section 19). This includes storage on a cloud the servers of which are located outside the UK.

6.7 Policy Actions

6.7.1 Fair and lawful processing

Fairness of processing means that we only process data in the manner in which data subjects reasonably expect. In order to make data subjects aware of how we process personal data, the UK GDPR requires that we provide data subjects with certain information when we collect information from them as well as when we collect information about them from other sources.

If personal data is collected directly from data subjects, we will inform them (in writing) about:

- Our identity and contact details;
- The identity and contact details of the Data Protection Officer;
- The purposes for which we intend to process the data and the legal basis for the processing;
- If data processing is justified on the basis of legitimate interests pursued, those legitimate interests should be identified;
- The recipients, or categories of recipients of the data;
- If we intend to transfer personal data out of the UK or to an international organisation, the fact that we shall transfer data in this manner and information about the safety of or safeguards involved in such transfer;
- The period for which the data will be stored or the criteria for determining that period;
- The rights of data subject as set out in Schedule 1;
- Where processing is based on consent, the right to withdraw that consent at any time;
- The right to complain to the Information Commissioner's Office;
- Whether the provision of personal data is a contractual or statutory requirement, the possible consequences of failing to provide it;
- The existence of any automated data processing (i.e. decisions made solely by an automated process, without human judgment, which significantly affects a Data Subject) and meaningful information about how the process works;
- If we intend to process personal data further for a purpose other than that for which the data was collected we will also provide information on that purpose prior to the further processing.

This information must be given at the time when the personal data is obtained.

If data is collected from a third party rather than directly from the data subjects, we will provide to the data subjects (in writing), within a reasonable time and not later than one month after we collect the data, with the information described above as well as the following information:

- The categories of data concerned;
- The source of the personal data.

If we use personal data collected in this manner for communicating with data subjects we must provide this information not later than the time of our first communication with them, and if we intend on disclosing any of the personal data we must provide this information before the disclosure.

If we collect data from the data subject and we are aware that we will later be collecting additional data from third party sources it may be more effective to provide all the information to the data subject when we collect the data from them.

The provision of information described above will not apply where the data referred to is collected by a member organisation or member church and is shared with the Union for the purpose of updating contact details to ensure Union records are accurate and up to date.

The information must be given in clear and plain language, and must be concise, transparent, intelligible and easily accessible. Depending on the context, it may be appropriate to provide the more essential information and explain where the full information can be found.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter, unless a legal exemption applies. Legal advice should be sought before an exemption is applied and a record must be kept of a decision to apply an exemption including the reasons for it.

Personal data received about a data subject from other sources may be a protected disclosure for whistleblowing purposes or may have been referred to us by an official authority to carry out our own investigation. The processing of complaints and allegations of criminal activity may be withheld from the data subject where one of the legal exemptions applies.

Processing of data is only lawful if at least one of the conditions listed in Article 6 of the UK GDPR is satisfied. These conditions include:

- The data subject has given consent to the processing of the data for specific purposes;
- The processing is necessary for a contract with the data subject;
- The processing is necessary for us to comply with a legal obligation;
- The processing is necessary for legitimate interests pursued unless these are overridden by the interests, rights and freedoms of the data subject.

The UK GDPR includes other conditions and before deciding on which condition should be relied upon, the original text of the UK GDPR should be consulted as well as any relevant guidance.

When we rely on the legitimate interests ground we must carry out a balancing exercise, weighing our legitimate interests with the rights of the individuals concerned. If our use of that information poses a risk to the rights of the individual it may be more appropriate to obtain the individual's consent for the particular processing so as to give the individual more control over how we use their information.

When special category personal data is processed, we must also satisfy one of the conditions set out in Article 9 of the UK GDPR. These include:

- The data subject has explicitly given consent;
- The processing is necessary for carrying out our obligations under employment and social security and social protection law;
- The processing is necessary for safeguarding the vital interests (in life or death situations) of an individual and the data subject is incapable of giving consent;
- The processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
- The processing is necessary for pursuing legal claims.

The UK GDPR provides other alternatives for processing special category personal data as well and before deciding on which condition should be relied upon, the original text of the UK GDPR should be consulted together with any relevant guidance

It is important that decisions we make concerning which grounds we will rely on are recorded.

6.7.2 Consent

Where personal data is not necessary for contractual purposes or for our legitimate interests or in the absence of a legal obligation justifying processing, usually the consent of the data subject is required to justify processing. Consent can however be withdrawn at any time and if withdrawn, the processing should cease. Data subjects should be informed of their right to withdraw consent and withdrawing consent should be as easy as it is to provide consent.

The UK GDPR requires consent to be a freely given, specific, informed and unambiguous indication of the data subject's wishes. It must be a statement or clear affirmative action which signifies agreement to the processing of personal data relating to the member. As a result, presumed consent and pre-selected opt-in boxes will not constitute valid consent under the UK GDPR.

Consent cannot be relied on if the individual concerned does not have a choice whether to provide us with their information or not. We cannot therefore require consent as a condition to providing a service as consent would not be considered to be freely given (other grounds for processing may be useful in such a case).

When obtaining consent we are also required to clearly set out the specific reason why we are obtaining the individual's information and how we intend to use it so that the individual's consent can be considered specific and informed.

Consent is not everlasting and before obtaining consent for processing personal data we should consider how we can ask the individual to refresh their consent at reasonable intervals in the future. Although the law does not specify how long consent is valid for, in determining this we will take into account how long the individuals concerned can expect their data to be used for. As an example, if we obtain consent from an individual to use their image that individual might reasonably not expect us to use their image more than a year later.

It is not enough that we obtain consent but we must be able to show that we obtained consent. It is therefore best to obtain consent in writing so that we can keep a clear and durable record of it.

6.7.3 Processing for specified purposes

We will only process personal data for the specific purposes set out in our privacy notices or for other purposes specifically permitted by law. We will notify those purposes to the data subject in the manner described above unless there are lawful reasons for not doing so and this is permitted by a legal exemption.

We may process data for further purposes which we might not have envisaged when providing the data subject with the original privacy notice as long as the further purpose is compatible with the original purpose for which the data was collected. When assessing compatibility, we will consider, among all other relevant issues, the link between the purposes, the context in which the data was collected, the reasonable expectation of the data subject concerned, the nature of the personal data, the consequences of the further processing and the existence of appropriate safeguards. We are required to inform data subjects of the further purposes and provide them with appropriate additional information before we commence the further processing.

6.7.4 Adequate, relevant and non-excessive processing

We will only collect and use personal data to the extent that it is required for the specific purpose described above (which would normally be notified to the data subject). We should collect and use just enough information, which is relevant, to achieve that purpose, but not more than is required.

We will check records regularly for missing information and to reduce the risk of irrelevant or excessive information being collected.

When implementing systems which involve processing personal data we will consider how such systems can provide for data minimisation by design and by default.

6.7.5 Accurate data

We will ensure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data should be checked at the point of collection and at regular intervals afterwards. If a data subject informs us of a change of circumstances their record must be updated as soon as is practicable. All reasonable steps will be taken to destroy or amend inaccurate or out-of-date data.

Data subjects are to be given the means to easily contact us to amend any data which we hold about them if it is inaccurate or outdated and we should affect such changes unless we have a good reason not to.

Where a data subject challenges the accuracy of their personal data, we will mark this information as potentially inaccurate and we will try to resolve the issue informally. Where the issue is not resolved, disputes will be referred to the Data Protection Officer.

Records should be kept in such a way that the individual concerned can inspect them. Such documents could also be required, in certain circumstances, to be disclosed to other bodies at a later date. Information should therefore be correct, unbiased (unless a professional opinion is required to be given), unambiguous and clearly readable. Information from an external source should be recorded clearly and dated, and the source identified.

6.7.6 Data retention and destruction

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and we will comply with official guidance issued to our sector with regard to retention periods for specific items of personal data. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

Information about how long we will keep records for can be found in our Data Retention Schedule.

When they are no longer required, solid state devices, hard disks, CD-ROMs and other storage media which have at any time held or processed personal data must be dealt with so that the personal information cannot be recovered from them. They should be overwritten using a process approved by our IT team so that the data previously stored on them is beyond recovery by any available technological or other means, or should be physically destroyed by secure means.

6.7.7 Processing in accordance with data subjects' rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any personal data held about them by us
- Prevent the processing of their personal data for direct-marketing purposes;
- Ask to have inaccurate personal data amended; and
- Object to processing, in certain circumstances.

If any communication is received by a member of staff from a data subject which relates or could relate to their data protection rights, this should be forwarded to our Data Protection Officer immediately.

A more detailed description of the rights of data subjects can be found in Schedule 1 although the precise conditions contained in the UK GDPR will be applied when giving effect to these rights.

6.7.8 Direct marketing

'Direct marketing' means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This includes contact made by organisations to individuals solely for the purposes of promoting their aims and the advertising need not be of a commercial product, nor need anything be offered for sale. We will adhere to the rules set out in the UK GDPR, the Privacy and Electronic Communications Regulations and any laws which may amend or replace the rules governing direct marketing when we make contact with data subjects, whether that contact is made by (but not limited to) post, email, text message, social media messaging, telephone (both live and recorded calls) and fax. Stricter rules apply to marketing by email and other electronic means including text messaging, social media messaging, fax and automated telephone calls.

Any direct marketing material that we send should identify us as the sender and should describe how an individual can object to receiving similar communications in the future.

Data subjects have a very strong right to object to any form of processing of their personal data for a direct marketing purpose. If an individual exercises their right to object we are required to cease processing for this purpose within a reasonable time.

6.7.9 Dealing with subject access requests

All data subjects have a right to obtain from us copies of personal data which we hold about them. Such copies shall be provided together with information about:

- The purposes of processing;
- The categories of personal data concerned;
- The recipients to whom the data has been or will be disclosed, particularly if these are outside the United Kingdom;
- The envisaged period for which the data will be held;
- The existence of the right to request rectification, erasure or restriction of processing as well as the right to object to data processing;
- The right to lodge a complaint to the ICO;
- Where the data is collected from someone other than the data subject, the source from which we obtained the data;
- The existence of any automated decision-making and a description of the logic involved as well as information about the significance and envisaged consequences of such processing;
- The safeguards in place in relation to personal data transferred outside the United Kingdom.

Requests do not need to be made in any particular form and need not quote the law or the right of subject access. It is enough that a data subject asks for their personal information. Staff who receive such a request must forward it to the Data Protection Officer immediately as there is a limited timeframe in which we are required to comply and we may need to obtain additional information from the individual before we can do so, including clarification of the scope of the request and confirmation of the individual's identity.

More information about the right of subject access can be found in Schedule 1.

We do not and cannot charge a fee for complying with a subject access request save in exceptional circumstances described in Schedule 1.

Except in limited circumstances when complying with a subject access request we may not disclose the personal data of third parties. For this reason personal data of third parties should be redacted from documents which are provided to the requester.

The right of subject access (SAR) is a right of the individual and is therefore only exercisable by that particular individual. The information should also only be provided to that individual. The exception to this rule is when a request is made by a person other than the data subject on behalf of the data subject and:

- The data subject has authorised the requester to make the request on their behalf and to receive the information; or
- The data subject is incapable of understanding the nature and implications of a subject access request.

With regard to requests made by children or on behalf of children, as a rule of thumb, a child of 12 or over is usually regarded as capable of possessing the requisite mental capacity, although this is not an absolute indicator and decisions in this regard will depend on the mental and emotional development of the child in question.

Where we have reasonable doubts as to the identity of the requester we will seek to verify their identity before any personal data is disclosed. Evidence of legal authority to act on behalf of the data subject will be required where a request is made on behalf of someone else.

Evidence of identity of the data subject and any third party acting on their behalf can be established by production of a combination of the following (in original or certified copy):

- Passport;
- Photo driving licence;
- Utility bill showing current address;
- Birth/marriage certificate;
- P45/P60.

Evidence of legal authority to act on behalf of an adult can include:

- Original signed letter of authority from the data subject (where the data subject possesses full mental capacity);
- Original or certified copy of a relevant power of attorney or Court of Protection Deputyship Order (where the data subject lacks mental capacity).

In certain circumstances, exemptions may apply which may require or allow us to withhold information requested in response to a subject access request although it should be presumed that all personal data relating to an individual should be disclosed to them. Legal advice should be sought when it is thought that an exemption may be applicable.

We will keep records of all subject access requests and a record of why information was redacted or withheld (e.g. subject to an exemption).

Further information on dealing with subject access requests can be found on the website of the Information Commissioner's Office (ICO).

6.7.10 Disclosures of information to third parties (data sharing)

- All personal data is held securely by us and will be treated in a confidential manner. We will only disclose personal data when we have legal grounds to do so and if we have previously informed the data subject about the possibility of similar disclosures (in a privacy notice), unless legal exemptions apply. Only authorised and properly instructed members of staff are permitted to make external disclosures of personal data. These disclosures may include:
- Disclosures made in accordance with a legal obligation, such as a court order or statutory duty;
- Disclosures made in order to enforce or apply any contract with the data subject; or
- Disclosures made to protect our rights, property, or safety of our employees, volunteers, contractors or others. This includes exchanging information for the purposes of the prevention or detection of crime.

We will keep records of all information supplied in response to a request for disclosure by a third party and will carefully document any exemptions which may have been applied (including the reasons for their application). Legal advice may need to be obtained in appropriate cases.

We will abide by the ICO's statutory Data Sharing Code of Practice (or any replacement code of practice) when sharing personal data with other data controllers.

6.7.11 Security of personal data

We will process personal data in a manner that ensures that it is kept appropriately protected and secure, including from unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical and organisational measures which include as a minimum those described below.

We will implement appropriate technical and security measures which ensure a level of security of processing which is appropriate to the risk of processing.

In assessing the appropriateness of technical and organisational measures we shall take into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context and purpose of processing;
- the risk (of varying likelihood and severity) for the rights and freedoms of natural persons.

In assessing the appropriateness of the level of security we shall, among other relevant considerations, take into account the risks that are presented by the processing involved, in particular the risks which could result from a personal data breach.

We will put in place policies, measures, procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. These may include:

- Pseudonymisation and encryption of personal data. Pseudonymisation is when personal data is processed in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information which is kept separately and subject to measures which ensure that personal data are not attributed to an identifiable individual;
- Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Measures to ensure that we are able to restore availability and access to personal data in a timely manner if there is a physical or technical incident;
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing.

The security measure we put in place include:

- Systems Security
    - Security software is installed on all computers containing personal and/or confidential data;
    - Only authorised users are allowed to access computer files and passwords are required to be both strong and regularly changed. Staff and others to whom systems access is granted should never share their password with any other person;
    - Only a limited portion of the personal information that we control will be available for all staff to use: most staff will have limited access to personal and confidential data – on a 'need to know', role-appropriate basis;
    - All non-portable user devices will be encrypted and so far as possible, portable devices such as laptops, memory sticks and portable hard drives will be encrypted;
    - Computer files are regularly backed up and copies kept securely;
    - Persons who process personal data on our behalf ('data processors') will be vetted before we appoint them and we will not appoint them unless we are satisfied that they are able to process data in a manner which meets the requirements of the UK GDPR and provides protection for the rights of data subjects. Data processors will only be engaged by means of written contracts which contain the provisions required by the UK GDPR;
- Organisational Security
    - Staff will undergo regular data protection training and must adhere to the terms of this policy and our Data Retention Policy
    - Staff and contractors shall be subject to a legally binding duty of confidentiality;
    - Staff and contractors must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended;
    - All paper documents containing personal data should be locked away in desks and cabinets and not left out overnight;
    - Paper documents which are required to be destroyed shall be securely shredded. Digital storage devices should be physically destroyed when they are no longer required;

6.7.12 Transferring personal data outside the United Kingdom (UK)

We may only transfer personal data we hold to a country outside the UK if this is permitted under the UK GDPR. This includes situations where we upload personal data to a cloud the servers of which are situated outside the UK.

Under the UK GDPR, we are permitted to transfer data outside the UK in certain circumstances. These include situations where we transfer data:

- To a country or international organisation which the UK government declares, by means of a decision, to be a country or international organisation which provides an adequate level of protection (provided that the relevant decision remains in force);
- Pursuant to a contract which incorporates standard data protection contractual clauses which are specified in regulations made by the Secretary of State in accordance with the UK GDPR;

- Pursuant to standard data protection contractual clauses (SCCs) which are issued by the ICO;
- The data subject explicitly consents to the transfer, which consent shall be of the level required in section 9 of this policy and the UK GDPR;
- The transfer is necessary for one of the reasons set out in the UK GDPR, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

Satisfying one of the conditions above does not eliminate the need to comply with all other requirements for processing personal data.

When we use the services of a cloud service provider (or any other data processor) which requires data to be processed outside the UK we must ensure that we satisfy one of the conditions contained in this section 19 of this policy (or alternatives provided under the UK GDPR) as well as comply with the requirements relating to the appointment of data processors.

6.7.13 Dealing with Data Protection breaches

Where staff or contractors working for us consider that this policy has not been followed the matter should be reported immediately to the Data Protection Officer. These include, among others, situations where:

- an unauthorised person may have gained access to personal data;
- personal data (including copies and backups of it) has been lost, even if temporarily;
- data has been uploaded onto an unsecure server, including a server situated outside the UK if this is not done in accordance with the relevant UK GDPR requirements;
- a computer or other device on which personal data is accessible is affected by a virus or other malicious code;
- personal data becomes corrupted or is accidentally altered;
- any login details were discoverable for a period of time;
- a direct marketing email is sent in a manner which allows recipients to view the email addresses of others;
- a power outage or other similar incident results in personal data not being accessible for a period of time.

We must keep records of personal data breaches, even if we do not report them to the ICO, and such records must be such as to enable the ICO to verity our compliance with the UK GDPR. The records will be kept by the Data Protection Officer and will describe, as a minimum:

- The facts relating to the personal data breach;
- Its effects; and
- Remedial action taken.

We are required to report all data breaches which are likely to result in a risk to any person, to the ICO. Reports must be made within 72 hours from when we become aware of the breach and the time limit starts to run from when any member of staff or contractor becomes aware of the breach and not when the Data Protection Officer becomes aware. For this reason it is very important that incidents are reported to the Data Protection Officer immediately so that he or she can decide if a report should be made.

Reports to the ICO shall contain the following information:

- A description of the personal data breach including the categories of and number of data subjects and records concerned;
- The name and contact details of the Data Protection Officer and other persons from whom the ICO can obtain more information;
- The likely consequences of the data protection breach;
- The measures taken or proposed to be taken to address the personal data breach including measures to mitigate the possible adverse effects.

In situations where a personal data breach causes a high risk to any person, we shall, in addition to reporting the breach to the ICO, inform the data subject whose information is affected, without undue delay. This can include situations where, for example, information containing bank account details is left unattended in a public place or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights. When informing data subjects, we will, as a minimum, provide them with the information described above.

Since the timeframe within which we must report personal data breaches could start to run from the moment a contractor becomes aware of a personal data breach, we must make sure that in all our contracts with contractors, we require them to provide us with the information listed above immediately upon discovering a potential breach, as well as to provide us with any additional information we may require to comply with our data protection obligations.

When a data protection breach occurs, the Data Protection Officer shall consider the following:

- Does this policy require amending?
- Should further guidance be issued about this policy?
- Do any members of staff require additional training or guidance?
- Is it appropriate to take disciplinary action?

6.7.14 Record Keeping

The UK GDPR requires that organisations not only comply with the law but are able to show that they comply with the law. It is therefore very important that we keep clear records of all processing activities and decisions we make concerning personal data (setting out our reasons for those decisions). Although the UK GDPR lists specific records which should be kept this does not reduce our responsibility to ensure that we are able to prove compliance with the law at all times.

The UK GDPR specifically requires that we keep, as a minimum, the following records about our processing activities:

- The name and contact details of any joint controller, any representative and/or Data Protection Officer;
- The purpose of the processing;
- A description of the categories of data subjects;
- A description of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed;
- Transfers to countries or organisations outside the UK (including their identification) and any relevant safeguards;
- The envisaged time limits for erasure of the different data;
- A description of security measures taken.

The UK GDPR also requires data processors to keep records and when appointing a data processor we shall require them, in the contract by which they are appointed, to keep such records and to give us access to such records when we require it.

6.7.15 Data Protection by design and by default

We will implement appropriate technical and organisational measures to ensure that all personal data is processed in accordance with the UK GDPR, primarily the principles of data protection described in this policy. This includes having safeguards built into our systems which provide for compliance by default. As an example, forms which we use for recording personal data should provide for inputting all relevant data but no extra information. This is referred to as data minimisation. Other measures include pseudonymisation which is described above and which increases the security of personal data.

6.7.16 Data Protection Impact Assessments

Before carrying out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles and data transfers outside the UK. We may also conduct a DPIA in other cases when we consider it appropriate to do so. Any decision not to conduct a DPIA should be recorded.

DPIAs should be carried out early enough to allow recommendations to be acted upon and a DPIA should be continuously be carried out on existing processing activities. A DPIA should be reassessed at least every three years, depending on the nature of the processing and the rate of change in the situation.

All DPIAs should involve the Data Protection Officer and his or her advice and decisions shall be documented.

When carrying out a DPIA we will consult with the data subjects concerned and if we decide not to do so we shall keep a record of such a decision (including reasons).

If we are unable to mitigate the identified risks such that a high risk remains we are required to consult with the ICO.

DPIAs shall be conducted in accordance with the ICO's guidance on Data Protection Impact Assessments.

Appointing data processors

When appointing a contractor who will process personal data on our behalf (a data processor) we will, before appointing them, carry out a due diligence exercise to ensure that the relevant processor will implement appropriate technical and organisational measures to ensure that the data processing will meet the requirements of data protection law, including keeping the data secure, and will ensure protection of the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do so.

We will only appoint data processors on the basis of a written contract which must contain provisions which require the processor to:

- Process the personal data only on our documented instructions;
- Ensure that persons authorised to process the personal data have committed themselves to confidentiality;
- Take all measures required in relation to security of processing;
- Not appoint sub-processors without our prior written authorisation and equivalent contractual obligations;
- Assist us to fulfil our obligations to give effect to the rights of data subjects;
- Assist us in complying with our legal obligations, in particular those relating to security, breach notification and communication with data subjects, and carrying out data protection impact assessments;
- At our choice, delete or return all personal data after the end of the provision of services relating to the processing, and delete existing copies unless longer storage is required by law;
- Make available to us all information necessary to demonstrate compliance with our obligations in relation to appointing data processors;
- Allow us to conduct, and assist us in conducting, audits, including inspections of the processors, which may be carried out by us or an auditor of our choosing;
- Inform us if an instruction we give to the processor breaches any data protection law.

In addition to the provisions listed above it may be appropriate for us to require a data processor to comply with our policies, maintain records, provide us with information and otherwise generally assist us to comply with our data protection obligations.

It should be noted that it is not enough to have the clauses listed above included in a contract with the processor and we will remain liable for breaches of data protection law committed by the data processor unless we can show that we were not in any way responsible for the event giving rise to the damage. We would not be able to show this unless we carry out the due diligence exercise mentioned above and unless we carefully monitor the data processing throughout the duration of the contract.

6.8 Changes to this policy

We reserve the right to change this policy at any time. Any amended versions of this policy will take effect from the time they are uploaded to our website. Where appropriate, we will notify data subjects of those changes by mail or by email.

7 Information Technology

7.1 Overview

The Association understands the good that comes from electronic communications and social networking. It is not our desire to create consternation or dampen creativity when it comes to the use of these media. At the same time, we recognise the tremendous potential for hurt and misunderstanding that go with these media. We trust that by following these guidelines and common sense, we are all able to both reap the rewards of electronic communications … and avoid their potential pitfalls.

The aims of this policy are:

To promote the professional, ethical, lawful and productive use of Association information technology (IT)

- To define and prohibit unacceptable use of Association IT
- To describe the responsibilities of staff using Association IT
- To outline disciplinary procedures that will apply to policy breaches

7.2 General Principles

Association IT is provided for business use.

Use of any Association IT for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this policy.

The Association reserves the right to monitor any aspect of its IT in order to protect its lawful business interests. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings.

Users should have no expectation of privacy when using Association IT.

Breach of this policy may result in disciplinary action. Depending on the severity of the breach, this may include:

- An informal warning from a manager
- A formal verbal or written warning for misconduct
- Dismissal for gross misconduct
- Criminal proceedings
- Civil proceedings to recover damages

7.3 Association Responsibility

The Association will keep a record of all owned equipment (laptops, projectors, audio / visual equipment etc). Such details will include make and model of the equipment, date of purchase, purchase price and serial number(s).

The Trustees will agree a spending limit for IT equipment, but it may be possible for a user to purchase a more expensive machine and pay the difference.

All Association owned equipment may be subject to audit (including all stored data) at any point in time by the Operations Manager or other person(s) appointed by the Trustees.

7.4 User Responsibility

All Association owned IT equipment must have the following set up on it to protect the user and any sensitive personal information which is stored about church members.

- Automatic downloading and applying of security update patches.
- Functioning and up to date Antivirus software.

- Ideally, Sensitive Personal Information should not be stored. If Sensitive Personal Information must be stored the data must be encrypted.
- Sensitive personal information must not be shared by email, or other electronic communication unless encrypted.
- All users of Association computer equipment information technology should store files on Microsoft OneDrive

All portable IT equipment must be protected with a password, which must not be shared. If compromised, a password should be changed immediately.

Passwords should be as secure as possible and should not be written down.

IT equipment should be kept secure and must not be left unattended when in a public environment. Ideally IT equipment should not be left unattended in a vehicle but when this is unavoidable it must be hidden from view.

All Association owned equipment must usually be returned on leaving a post, but it may be possible for users to purchase their equipment dependent on operational needs

7.4.1 Use of the Internet

The Association values the potential good that comes from web pages, social networking pages, blogs, texting, instant messaging, e-mail and other forms of electronic social networking / communication. Simultaneously we recognise that misunderstanding, personal offense, hurt, legal exposure and damage to the Association can potentially accompany use of these media. All workers are to abide by the following communication guidelines.

Internet access should be limited to appropriate Association use only. For example, visiting pornographic adult sites and gambling sites is totally prohibited.

Use of the Internet in attempts to gain unauthorized access to remote systems is prohibited.

7.4.2 Ensure integrity

Electronic communications should be consistent with the teaching of scripture and the values of the Association.

Nothing should be written online that would not be said in person as a representative of the Association.

Staff are expected to have the foresight to anticipate, within reason, how their words and/or actions may be perceived by their audience and to those under their care. It is highly recommended that any potentially difficult posting should be reviewed by an Association colleague.

7.4.3 Promote credibility

Facts should be checked to ensure they are correct; in proper context and that positions are justifiable. Response to those who disagree should be in a spirit of love and grace.

Electronic communications should not be used to resolve interpersonal / church conflicts that are best handled face-to-face. It is highly recommended that any potentially difficult posting should be reviewed by an Association colleague before sending.

7.4.4 Keep confidences and avoid libel

Communications should not inadvertently share confidential information (sometimes we deal with a lot of confidences in Association work so extra care must be taken with this). With any public postings the author is legally liable for what is written. Laws governing slander, libel, defamation and copyright apply. Outside parties can pursue legal action against individuals for postings.

7.4.5 Do not engage in polarising political speech

As a charity we cannot be seen to endorse or support political candidates. Nothing in public communications should lead people to believe that the Association is endorsing a political candidate or party.

Any public posting on a political issue, which is made speaking on behalf of the Association must be agreed by the Team Leader or Company Secretary.

It is recognised that Association staff may wish to speak in their own right on political issues when posting blogs, Facebook postings, tweets etc., but they should make it clear that this is their own view and not necessarily the view of the Association and Association IT platforms should not be used in these cases.

7.4.6 Respect the Association and its staff

Since electronic communications are public (or easily made public), we expect everyone associated with us to be respectful to Association workers. Any member of staff who uses electronic communications to disparage the name or reputation of the Association, its practices, or its ministers, officers, employees or volunteers will be subject to discipline, up to and including immediate termination of employment.

7.4.7 Limit expression in written words

Written words can easily convey the wrong message as they do not have the “non-verbal” channels that accompany face-to-face communication - body language, facial expressions and tone of voice that can help ensure proper context are missing. Staff should re-read everything prior to sending to check if there is any possibility of misunderstanding and consult a colleague if in any doubt.

7.4.8 Specific guidance for communication with children and vulnerable adults

All interaction via social media sites with children and vulnerable adults should be via the Association’s platform accounts and not through the any Association staff’s personal individual platform accounts.

It is the Association’s default practice not to make one on one connections with young people through social media, though it is acknowledged that this is a useful communication tool. On rare occasions it might be necessary, but this should be for a specific purpose and then the conversation terminated. It is expected that each sub-group within the association will find its own way of using social media to communicate within the law and in a way that is a positive, safe, experience for all members of the group.

7.5 Personal Use

The Association recognises that personal access the web at work helps employees to maintain a positive work life balance.

Limited and ‘reasonable’ personal use of the web is permitted. Reasonable use is defined below. Personal use of all other systems is prohibited.

Web access may be monitored to ensure compliance with policy. Employees that choose to make personal use of Union systems do so in acceptance of the monitoring measures outlined in this policy.

Personal use of these systems is a privilege. The Association reserves the right to withdraw it either individually or globally at any time without notice or explanation.

7.6 Sensitive Information

The following is information that the Association believes is Sensitive Personal Information (and needs protecting as stated in the Association IT policy.

- The Association Church / Ministers Directory and all databases (including the Baptist Union “thankQ” and “MIX”).

- Church Elders / Deacons / Leadership/Member's Minutes from our churches.
- Correspondence from and to all The Association Ministers.
- Any personal file that a member of Association staff might keep on Ministers or churches.
- Association and local church financial information.
- All Association Safeguarding matters.

8 Appendix 1 - Safeguarding

8.1 Association Contacts

Association Safeguarding Officer: Wendy Mann

They will support other regional team members and churches, providing advice and guidance on how to manage safeguarding concerns. This includes supporting churches to put Safeguarding Contracts in place, assisting with safeguarding risk assessments and promoting excellence in safeguarding in all Baptist churches in their regional area.

Contact Details: 07545 686143
safeguarding@seba-baptist.org.uk

Deputy Association Safeguarding Contact: Revd Paul Kerley

If the Association Safeguarding Officeris on leave or unavailable, then the Deputy Safeguarding Contact will be available to fulfil their role

Contact Details: 01580 766020 / 07821 550038
paul@seba-baptist.org.uk

Association Safeguarding Trustee: Revd Jonathan Hardwick

They will raise the profile of safeguarding amongst the trustees of the Association and oversee the implementation of the safeguarding policy and procedures on behalf of the trustees.

Contact Details: 01883 742825 / 07528 461112
earlswoodbc@btinternet.com

8.2 Police and Local Authority Contacts

The Regional Association spans county boundaries. This means that we are likely to be liaising with police and social services from a number of authorities.

The Police Forces working within the Regional Association area are:

Force Name	Areas covered
1. Kent Police	Kent
2. Sussex Police	East and West Sussex
3. Surrey Police	Surrey
4. Hampshire Constabulary	Hampshire

The Local Authorities working within our Regional Association boundaries are:

Local Authority	LADO contact details	Children's Services (MASH, Assessment and Intake team) Contact Details	Adult Services (MASH, Assessment and Intake Team) Contact Details
Kent	03000 41 08 88 kentchildrenslado@kent.gov.uk	03000 411111 www.kscmp.org.uk	03000 416161 social.services@kent.gov.uk
West Sussex	Claire Coles / Sally Arbuckle 01403 229900 LADO@westsussex.gov.uk	01403 229900 / 0330 222 7799 MASH@westsussex.gov.uk	01243 642121 Emergencies 033 022 27007 www.westsussex.gov.uk/social-care-and-health/social-care-support/adults/raise-a-concern-about-an-adult
East Sussex	01323 464222 01273 335905/6 0-19.SPOA@eastsussex.gov.uk	01323 464222 / 01273 335905/6 0-19.SPOA@eastsussex.gov.uk	0345 60 80 191 / 01323 636399
Brighton and Hove	01273 295643 / 07795 335879 darrel.clews@brighton-hove.gcsx.gov.uk	01273 290400 FrontDoorForFamilies@brighton-hove.gcsx.gov.ukk	01273 295555 accesspoint@brighton-hove.gov.uk
Surrey	0300 470 9100 / 0300 470 9100 LADO@surreycc.gov.uk	0300 470 9100 out of hours 01483 517898 csmash@surreycc.gov.uk	0300 200 1005 contactcentre.adults@surreycc.gov.uk
Hampshire	01962 876364 child.protection@hants.gov.uk	0300 555 1384 / 0300 555 1373 childrens.services@hants.gov.uk	0300 555 1386 / 0300 555 1373 adult.services@hants.gov.uk

8.3 Procedures for managing concerns and allegations

The Regional Association Safeguarding Officeris responsible for ensuring that churches within the association have access to support and guidance when managing safeguarding issues within their congregation. In addition, the role of the Association Safeguarding Officeris to both support and challenge church leaders where there are concerns about their approach to safeguarding, working with them to attain best safeguarding practice.

There may be occasions when the Association will take the lead in investigating a situation and these will be set out within these procedures. The Association Safeguarding Officerwill seek additional support and advice from the BUGB Safeguarding Team and other professionals when necessary. They will maintain a record of all concerns brought to their attention using a Case Record Sheet (Appendix B) and a Case Spreadsheet (Appendix C). All information collected and processed in this way will be held for at least 75 years in line with the BUGB Guide to Safeguarding Recording Keeping.

8.3.1 Concerns raised about SEBA workers

8.3.1.1 Regional Ministers

In the case of a Regional Minister the procedures below relating to BUGB Accredited Ministers will be followed.

8.3.1.2 Other staff, trustees and volunteers

If a safeguarding concern is raised about a member of staff, a volunteer or trustee working directly for the Regional Association then the Association Safeguarding Officerwill contact statutory services for advice on next steps, as well as seeking advice from the National Safeguarding Team. If the concern relates to a child or young person, the Local Area Designated Officer (LADO) will be contacted in the first instance. If the concern relates to an adult at risk then the Adult Safeguarding Team will be contacted. In both cases if there is a concern that criminal offences have or may have been committed the Police will be contacted in the first instance.

8.3.2 Concerns raised about BUGB Accredited Minister/Worker

When a member of the Regional Team is advised of a safeguarding concern involving an Accredited Baptist Minister they will contact the BUGB Safeguarding Team or the BUGB Ministries Team Leader within 24 hours, passing over all information they have received about the case.

The BUGB Safeguarding Team and Ministries Team Leader will agree a strategy for investigation, this will include decisions about who will make the referral to statutory agencies, whether suspension is required and when the person of concern can be informed of the issues that have been raised.

The Regional Minister will work with the national specialist teams (Safeguarding and Ministries) to ensure that information is shared in a timely manner to enable the investigation to progress. They will be led by the national team and will not disclose information to the person of concern or a third party without their agreement.

Pastoral Support

The Regional Association will offer pastoral support to the person of concern. This will not be provided by the Association Safeguarding Officerbut by another member of the Regional Team or an experienced minister from another church within the Association.

8.3.3 Concerns raised about a Regionally Recognised Pastor/Worker

When a member of the Regional team is advised of a safeguarding concern involving someone who is Regionally recognised, the responsibility for investigating lies with the Association Safeguarding Contact, with support from the National Safeguarding Team if needed. On occasions the Association may decide to subcontract the investigation to a third party such as 31:8 or an independent safeguarding consultant. However, the Association remains responsible for ensuring that the outcome of the investigation is acted upon and the advice given is followed.

The Regional Association Safeguarding Officerwill work closely with the statutory authorities. If the concern related to a child or young person the Local Area Designated Officer (LADO) will be contacted in the first instance. If the concern relates to an adult at risk then the Adult Safeguarding Team will be contacted. In both cases if there is a concern that criminal offences have or may have been committed the Police will be contacted in the first instance.

8.3.4 Concerns raised about an Unaccredited Minister or Pastor

If safeguarding concerns are raised about an unaccredited minister or pastor these should be managed by the trustees of the church in the first instance. The Association's role in this situation will be to support the church with the investigation. They will involve the National Safeguarding Team if necessary.

Although the Association will offer support, the church will need to take the lead in contacting statutory services. If the concern related to a child or young person the Local Area Designated Officer (LADO) will be contacted in the first instance. If the concern relates to an adult at risk then the Adult Safeguarding Team will be contacted. In both cases if there is a concern that criminal offences have or may have been committed the Police need to be contacted by the church in the first instance.

The Association will not be directly able to offer pastoral support to the person under investigation, however they may be able to recommend someone else to the church who can perform this role during the investigation.

8.3.5 Concerns raised by a church about the behaviour or well-being of someone who attends the church

The Association recognises that at times churches need additional support and advice when they have concerns about someone within their care. The Association Safeguarding Contact, or appointed Safeguarding Officers will offer this support and work with the church Designated Person for Safeguarding, consulting with the National Safeguarding Team when necessary. As with unaccredited ministers, the church will take the lead in contacting statutory agencies and undertaking the investigation.

To ensure that the correct advice is given to the church the Association Safeguarding Officerwill check whether the individual is in a position of leadership or trust within the church. If they are, the church will be asked to contact the LADO or Adult Safeguarding Team to seek their advice before the Association issues further advice.

8.3.6 Safeguarding Contracts

A Safeguarding Contract should be put in place by a church when they are aware that someone is either under investigations for, or has convictions for, offences against children or adults at risk. The Association will hold the template Safeguarding Contract and work with the church to ensure that the final agreement is robust and in line with the recommendations made by the National Safeguarding Team. The Association will hold a copy of the contract and work with the church to ensure that it is regularly reviewed. The Association Safeguarding Officerwill take an active role in facilitating contract meetings between the church and the subject of the contract. This is in line with the guidelines published by the National Safeguarding Team in the guide Safeguarding Contracts: Frequently Asked Questions, which is downloadable from the BUGB website.

If a church is reluctant to follow the safeguarding advice given by the Regional Association, then the Regional Safeguarding Contact will consult with the National Safeguarding Team and a decision made together about the best way to ensure effective safeguards are in place within the church.

8.3.7 Pastoral Care in safeguarding situations

When safeguarding situations occur within a church all those involved will inevitably need additional support and care. This includes the person making an allegation and the person subject to it. The Association will support the church in identifying people who can take on this pastoral role and on occasions may be able to seek support from a different church if they consider that this would be the most appropriate way forward.

8.4 The role of Association Safeguarding Officer

- To provide a first point of contact for advice when a safeguarding issue arises in a church
- To offer advice and guidance on the application of safeguarding policy and procedures at church level, including the involvement of statutory authorities as appropriate
- To offer on-going support to churches managing a safeguarding issue
- To challenge church leaders and trustees when good safeguarding practice is not in place
- To work collaboratively with the National Safeguarding Team to support our churches with complex safeguarding matters
- To promote excellence in safeguarding amongst Association colleagues and member churches
- To work collaboratively with other ASCs as part of the National Safeguarding Contacts Group and contribute to the development, implementation and review of safeguarding policies, procedures and projects at a national level.

8.5 Safeguarding Case Contact Sheet

STRICTLY CONFIDENTIAL

Referrer Name			
Referrer Position			
Referrer Phone No.		Email:	
Church Name			
Association			
Person of Concern Details	Name		DOB
	Address	Phone No.	Email
Alleged Victim / Victim Details	Name		DOB
	Address	Phone No.	Email
Situation			
Action taken			
Next steps needed			
People to inform			
Name			
Date			
Date for File Destruction			

Additional Contact Notes

Date	**Details of Additional Contact / Action taken**	**Initials**
	Continue as necessary	

9 Appendix 2 - Employment

9.1 Code of Conduct

9.1.1 Background

This Code of Conduct sets out standards of behaviour expected by the Association of all staff who are required to agree to the BUGB Declaration of Principle and Five Core Values. Conduct both in and out of work should be consistent with our objectives and the principles set out in those documents.

Staff are encouraged to make every effort to meet the standards of personal conduct and working practice set out in this code of conduct.

It is understood that while every member of staff is vulnerable to behaviour which contravenes that laid out in Scripture, our desire as an organisation is to inspire, encourage and build one another up in the faith in order to honour, obey and glorify God in our work.

This code of conduct seeks to facilitate this aim.

9.1.2 Behavioural Standards

Further to the acceptance of our Declaration of Principle and BUGB Five Core Values, we expect certain behavioural standards, examples of all staff which are:

- a willingness to give an account of their faith within an appropriate context in light of their particular responsibilities;
- regular commitment and participation in the life of a local Church; and
- treatment of those they deal with, with grace, respect, courtesy, politeness, forgiveness and Christian love.

9.1.3 Code of Conduct

A non-exhaustive list of matters which are considered to be gross misconduct is set out in the disciplinary procedure. There may be instances where inappropriate conduct inside or outside of formal working hours may also necessitate disciplinary action. Such issues may be as the result of an incapacity or an error of judgement rather than lifestyle choice or pre-determined behavioural choice.

The following is a non-exhaustive list of conduct which, although it may occur outside of formal working

hours we consider to be inappropriate for our employees and may lead to disciplinary action or dismissal:

- where it relates to a serious criminal offence;
- where it renders the employee unsuitable for the type of work they do e.g. someone who works with children found guilty of child abuse;
- where it leads to a breach of mutual trust between employer and employee e.g. accountant found guilty of fraud;
- where it is damaging to the reputation of the organisation for example:
    - Drunkenness or the use of illegal drugs
    - Use of obscenities, coarse jokes, gossip and slander
    - Any form of dishonesty including stealing and lying
    - Sexual immorality including adultery, deliberate viewing of pornography
    - Involvement in the occult or witchcraft
- where it affects the performance of the employee in their particular role e.g. a driver who loses his/her licence where driving is an essential occupational requirement; or

- where it relates to an employee’s acceptance of the Declaration of Principle and Five Core Values
    - e.g membership of a group who could oppose the principles set out in those documents or expressing views which are contrary to them.

9.1.4 Our Approach to Misconduct

Employees will be treated within a context of grace and compassion while time is taken to consider the circumstances of the situation e.g.

- The severity of the perceived misconduct.
- Whether the incident is a 'one-off ' or part of repeated behaviour or lifestyle.
- Whether the behaviour breaches our safeguarding policies and procedures
- Any mitigating circumstances e.g. personal issues.
- The position of trust of the employee.
- The particular duties of the employee.
- Christian maturity and understanding.
- The treatment of similar instances of misconduct by other employees.
- The employee's length of service.
- The extent of any 'live' disciplinary warnings.
- Evidence of repentance.

9.2 Supervisory Meetings

All supervisory or support meetings should be recorded by completing this form. This is to provide a record and stimulus for regular discussion of the employee's progress and development.

The line manager should complete this form after each supervisory meeting and send it to the employee for their agreement as a fair record of any decision made. A copy of the form should be kept in eth employees HR record.

Complete boxes as relevant:

Name of Employee		**Name of Line Manager**	
Date and Time		**Meeting Format** *(delete as appropriate)*	Face-to-Face / Phone / Email
Review of any actions from the last supervisory meeting			
Topics for Discussion			
Development Needs Identified			
Actions set for the next meeting			
Date of Next Meeting			
Signature of Line Manager			
Signature of Employee			

9.3 Procedures

9.3.1 Capability Hearings

The aims of a capability hearing will usually include:

- setting out the required performance standards that we believe the employee may have failed to meet, and going through any relevant evidence that the Association has gathered;
- allowing the employee to ask questions, present evidence, call witnesses, respond to evidence and make representations;
- establishing the likely causes of poor performance including any reasons why any measures taken so far have not led to the required improvement;
- identifying whether there are further measures, such as additional training or supervision, which may improve performance;
- where appropriate, discussing targets for improvement and a time-scale for review;
- if dismissal is a possibility, establishing whether there is any likelihood of a significant improvement being made within a reasonable time and whether there is any practical alternative to dismissal, such as redeployment.

A hearing may be adjourned if we need to gather any further information or give consideration to matters discussed at the hearing. You will be given a reasonable opportunity to consider any new information obtained before the hearing is reconvened.

The Association will inform the employee in writing of its decision and its reasons for it, usually within one week of the capability hearing. Where possible the Association will also explain this information to the employee, in person.

9.3.2 Stage 1: Capability Hearing [improvement note]

Following a Stage 1 capability hearing, if the Association decides that the employee's performance is unsatisfactory, the employee will be given an improvement note, setting out:

- the areas in which they have not met the required performance standards;
- specific targets for improvement;
- any measures, such as additional training or supervision, which will be taken with a view to improving performance;
- a period for review;
- the consequences of failing to improve within the review period, or of further unsatisfactory performance.

An improvement note may be authorised by the Company Secretary.

The improvement note will normally remain active for six months from the end of the review period, after which time it will be disregarded for the purposes of the capability procedure. However, a permanent record of it will be placed on the employee's personnel file.

The employee's performance will be monitored during the review period and the Association will write to the employee to inform them of the outcome:

- if the employee's manager is satisfied with the employee's performance, no further action will be taken;
- if the manager is not satisfied, the matter may be progressed to a Stage 2 capability hearing; or
- if the manager feels that there has been a substantial but insufficient improvement, the review period may be extended.

9.3.3 Stage 2: Capability Hearing final written warning

If the employee's performance does not improve within the review period set out in a first improvement note, or if there is further evidence of poor performance while the employee's improvement note is still active, the Association may decide to hold a stage 2 capability hearing. The Association will send the employee written notification as set out above.

Following a Stage 2 capability hearing, if the Association decides that the employee's performance is unsatisfactory, it will give the employee a final written warning, setting out:

- the areas in which the employee has not met the required performance standards;
- specific targets for improvement;
- any measures, such as additional training or supervision, which will be taken with a view to improving performance;
- a period for review;
- the consequences of failing to improve within the review period, or of further unsatisfactory performance.

A final written warning may be authorised by the Company Secretary.

A final written warning will normally remain active for six months from the end of the review period, after which time it will be disregarded for the purposes of the capability procedure. A record of the warning will form a permanent part of the employee's personnel record.

The employee's performance will be monitored during the review period and the Association will write the employee to inform them of the outcome:

- if the employee's manager is satisfied with his/her performance, no further action will be taken;
- if the employee's manager is not satisfied, the matter may be progressed to a Stage 3 capability hearing; or
- if the manager feels that there has been a substantial but insufficient improvement, the review period may be extended.

9.3.4 Stage 3: Capability Hearing dismissal or redeployment

The Association may decide to hold a stage 3 capability hearing if we have reason to believe:

- the employee's performance has not improved sufficiently within the review period set out in a final written warning; or
- the employee's performance is unsatisfactory while a final written warning is still active; or
- the employee's performance has been grossly negligent such as to warrant dismissal without the need for a final written warning.

The Association will send the employee written notification of the hearing as set out above.

Following the hearing, if the Association finds that the employee's performance is unsatisfactory, the Association may consider a range of options including:

- dismissing the employee;
- redeploying the employee into another suitable job at the same or a lower grade; or
- extending an active final written warning and setting a further review period (in exceptional cases where the Association believes a substantial improvement is likely within the review period)
- giving a final written warning (where no final written warning is currently active). The decision may be authorised by the Company Secretary.

Dismissal will normally be with full notice or payment in lieu of notice, unless the employee's performance has been so negligent as to amount to gross misconduct, in which case the Association may dismiss the employee without notice or any pay in lieu.

9.3.5 Appeals against action for capability.

If the employee feels that a decision about capability under this procedure is wrong or unjust they should appeal in writing, stating his/her full grounds of appeal, to the Company Secretary within one week of the date on which they were informed in writing of the decision.

If the employee is appealing against dismissal, the date on which dismissal takes effect will not be delayed pending the outcome of the appeal. However, if the employee's appeal is successful they will be reinstated with no loss of continuity or pay.

If the employee raises any new matters in their appeal, the Association may need to carry out further investigation. If any new information comes to light, the Association will provide the employee with a summary including, where appropriate, copies of additional relevant documents and witness statements. The employee will have a reasonable opportunity to consider this information before the hearing.

The employee will be given a written notice of the date, time and place of the appeal hearing. This will normally be two to seven days after they receive the written notice.

The appeal hearing may be a complete re-hearing of the matter or it may be a review of the fairness of the original decision in the light of the procedure that was followed and any new information that may have come to light. This will be at the Association's discretion depending on the circumstances of the employee's case. In any event the appeal will be dealt with as impartially as possible.

Where possible, the appeal hearing will be conducted by a manager who was not previously involved in the case and the manager who conducted the capability hearing will also usually be present. The employee may take a companion with them to the appeal hearing.

A hearing may be adjourned if the Association needs to gather any further information or give consideration to matters discussed at the hearing. The employee will be given a reasonable opportunity to consider any new information obtained before the hearing is reconvened.

Following the appeal hearing the Association may:

- confirm the original decision; or
- revoke the original decision; or
- substitute a different penalty.

The Association will inform the employee in writing of its final decision as soon as possible, usually within one week of the appeal hearing. Where possible this will also be explained to the employee in person. There will be no further right of appeal.

9.4 Procedure at disciplinary hearings

At the meeting the following procedure will be employed.

- Statement of complaint
  The Association will set out what the complaint against the employee is and go through the evidence gathered during the course of the investigation.
- **The employee's reply**
  The employee will be given the opportunity to state their case and respond to any allegations made. The employee will be allowed to ask questions and confer with their companion. If the employee accepts that they have done something wrong, steps may be agreed to remedy the situation.
- **General questioning and discussion**
  The person responsible for conducting the meeting may ask the employee for an explanation and will consider whether there are any specific, mitigating circumstances which should be taken into account. If the employee provides sufficient explanation, the proceedings will be brought to a close. If new facts occur at

this stage, it may be appropriate for the Association to adjourn the meeting and investigate the matter further before calling the employee back to the adjourned meeting.

- **Summing up**
  At this stage the person responsible for holding the disciplinary meeting should summarise the main points of discussion. The employee will be given the opportunity to add anything further.
- **Adjournment before decision**
  The meeting will be adjourned before a decision is made about the appropriate action. Following the meeting, a decision will be made as to whether or not disciplinary action is justified. Once a decision is made, the employee will be informed in writing within seven days.

Before deciding what, if any, disciplinary action is appropriate, consideration will be given to:

- whether the organisation's rules indicate clearly the likely penalty, as a result of the particular misconduct; (see Capability Hearing document – stage 3);
- whether the standards of performance demonstrated by other employees are considered to be acceptable, and whether the employee in question is not being singled out;
- the employee's disciplinary record (including current warnings), general work record, work experience, position and length of service;
- the reasonableness of the proposed penalty in the circumstances; and
- whether training, additional support or adjustments to the work are necessary to accompany any disciplinary action.

The employee will be given details of any disciplinary action as soon as a decision is made.

9.4.1 First formal action – unsatisfactory performance

In such cases, the employee will be given an "IMPROVEMENT NOTE" setting out:

- the performance problem;
- the improvement that is required;
- the timescale for achieving that improvement;
- a review date; and
- any support, including any training that the Association will provide to assist the employee.

The employee will be informed that the note represents the first stage of a formal procedure and is equivalent to a first "written warning". The employee will also be informed that failure to improve could lead to a final written warning and dismissal.

A copy of the note will be kept and used as the basis for monitoring and reviewing performance over a specified period.

If the employee's unsatisfactory performance, or continued unsatisfactory performance, is sufficiently serious (e.g. where it is having / likely to have a serious harmful effect of the organisation) the employee may be issued directly with a final written warning.

9.4.2 First formal action – misconduct

In cases of misconduct, depending on the seriousness of the misconduct, the employee may be given an improvement note setting out the nature of the misconduct and the change in behaviour required.

The warning will also inform the employee that a final written warning may be considered if there is further misconduct. A record of the warning will be kept by the Association but it will be disregarded for disciplinary purposes after 12 months.

9.4.3 Final written warning

Following the issue of a written warning, if there is still a failure to improve and conduct or performance remains unsatisfactory, or if the misconduct is sufficiently serious to warrant only one written warning, a FINAL WRITTEN WARNING will be given to the employee. This will give details of the complaint and will warn that dismissal will result if there is no satisfactory improvement, or if further misconduct occurs. The final written warning will advise the individual of the right of appeal. A copy of this final written warning will be kept by the Association but it will be disregarded for disciplinary purposes after 12 months (in exceptional cases the period may be longer) subject to satisfactory conduct and performance.

9.4.4 Dismissal

If conduct or performance is still unsatisfactory and the employee still fails to reach the prescribed standards, DISMISSAL will normally result. The employee will be provided as soon as reasonably practicable with written reasons for dismissal, the date on which employment will terminate and advised of their right of appeal within a specified time.

9.4.5 Gross misconduct

The following list is not exhaustive but provides examples of offences which are normally regarded as gross misconduct:

- verbal, physical, sexual or financial abuse of members of the Association;
- theft, fraud, deliberate falsification of records;
- serious breach of confidentiality;
- fighting, assault on another person or bullying;
- deliberate damage to the Association's property;
- serious incapability at work through alcohol or being under the influence of illegal drugs;
- serious negligence which causes unacceptable loss, damage or injury;
- serious act of insubordination;
- serious misuse of the Association’s property;
- bringing the Association into serious disrepute;
- a serious breach of health and safety rules;
- a serious breach of confidence;
- failure to adhere to the Statement of Faith required of all members of the Association;
- deliberately accessing internet sites containing offensive or obscene material;
- unlawful discrimination or harassment;
- failure to maintain one’s personal life in conformity with a good Christian testimony.

If the employee is accused of an act of gross misconduct, they may be suspended from work on full pay, while the Association investigates the alleged offence and pending the outcome of any disciplinary hearing. If, on completion of the investigation and a subsequent disciplinary hearing, the Association is satisfied that gross misconduct has occurred, the result will normally be summary dismissal without notice or payment in lieu of notice.

9.4.6 Appeals

An employee who wishes to appeal against a disciplinary decision should put their decision to appeal and the grounds of their appeal in writing to the Company Secretary within five working days of the date they were first notified of the decision. The employee has the statutory right to be accompanied by a colleague or a trade union representative to an appeal meeting.

The appeal shall, where possible, be heard by the deacons whose decision shall be final, subject to any overriding decision of the Association Meeting.

The employee will be informed in writing of the outcome of the appeal hearing as soon as possible. This will usually be within 10 working days.

9.5 Grievance Procedure

The employee should firstly raise any grievance informally with their supervisor, who in most cases, will be best placed to respond to their complaint. If the employee's grievance concerns their supervisor, they should instead raise their grievance with the Company Secretary.

9.5.1 Step 1

If, however, the matter cannot be satisfactorily resolved informally, the employee should raise the matter formally, in writing, giving full details of the nature of the employee's grievance, with their supervisor or the Association treasurer if their grievance is against their supervisor. Where an employee has difficulty expressing themselves because of language or other difficulties, they may seek help from their manager or the Company Secretary.

When stating their grievance, an employee should focus on preparing a factual account of their grievance.

9.5.2 Step 2 Meeting

The supervisor will invite the employee to a hearing in order to discuss the grievance as soon as reasonably practicable. The supervisor will ensure that the meeting will be held in private and the employee should make every effort to attend. The employee has the right to be accompanied by a companion.

9.5.3 Right to be accompanied at hearings

You may bring a companion to any capability hearing or appeal hearing under this procedure. The companion may be a fellow employee. You must tell the manager conducting the hearing who your chosen companion is, at least 24 hours before the hearing.

Employees are allowed reasonable time off from duties without loss of pay to act as a companion. There is no duty on employees to act as a companion if they do not wish to do so.

If the chosen companion will not be available at the time proposed for the hearing the employee may request that the hearing be postponed to a day not more than five working days after the day proposed by the Association. If the time proposed is reasonable, and the employee representative is able to attend, the hearing will be postponed until that time.

Whilst the companion may address the hearing and confer with the individual during the hearing, they do not have the right to answer questions on the part of the individual.

If your choice of companion is unreasonable, we may require you to choose someone else, for example:

- if in our opinion your companion may have a conflict of interest of may prejudice the hearing; or
- if your companion works at another site and someone reasonably suitable is available at the site at which you work; or
- if your companion is unavailable at the time a hearing is scheduled and will not be available for more than five working days.

We may, at our discretion, allow you to bring a companion who is not an employee (for example, a member of your family) where this will help overcome a particular difficulty caused by a disability, or where you have difficulty understanding English. At the meeting the supervisor will invite the employee to detail their grounds of grievance and consult with them on how it may be resolved.

We may adjourn the meeting if we need to carry out further investigations, after which the meeting will usually be reconvened.

The supervisor will adjourn the meeting before any decision is taken about how to deal with an employee's grievance. The supervisor will tell the employee when they can reasonably expect a response, if one cannot be made at the time. Usually, the supervisor will confirm any decision or proposed action to the employee in writing within 10 working days of the hearing. If it is not possible to respond within the specified time period the employee will be given an explanation for the delay and told when a response can be expected. The supervisor will set out clearly in writing any action that is to be taken and the employee's right of appeal. Where an employee's grievance is not upheld, the supervisor will explain the reasons.

9.5.4 Appeals

If the employee is dissatisfied with the outcome of the first meeting, they should appeal in writing to the Company Secretary stating their full grounds of appeal, within one week of the date on which the decision was sent or given to them. The Company Secretary will arrange a further meeting with deacons who have not previously been involved in the case. The employee has the right to be accompanied by either a colleague or a trade union representative.

Following the hearing, the employee will be informed of the decision or proposed action. This decision will be final subject to any overriding decision by the Association Meeting. If it is not possible to respond within the specified time period the employee should be given an explanation and told when a response can be expected. There is no further right of appeal.

10 Appendix 3 – Finance

10.1 Mileage and subsistence payments

Our standard rates for mileage and subsistence payments are shown below:

MILEAGE AND SUBSISTENCE	RATES
Mileage rate for the first 10,000 miles of business travel	45p per mile
Mileage rate for any business travel above 10,000 miles in one calendar year	25p per mile
Lunch allowance (when staff are working away from their normal place of work and need to purchase lunch)	Up to £8.00
Evening meal allowance (when staff are working away from their normal place of work and need to purchase an evening meal). This applies when staying away overnight or when the member of staff will not reach home until after 8.00pm.	Up to £12.00

10.2 Expenses Form

NAME:

DATE:

Date	Details	Dept /Project /Fund	Distance (miles)	Travel (mileage & parking)	Subsistence	Postage, printing & stationery	Sundry exps (eg petty cash)	Phone	Equipment eg tools or training aids	Other
Quickbooks code (for ref only)										
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
				£ -						
TOTALS				£ -	£ -	£ -	£ -	£ -	£ -	0

TOTAL BEING CLAIMED **£ -**

Notes

1 *Expenses can be handwritten or typed*
2 *Complete name, date and expense details in grids*
3 *Print and attach receipts*
4 *Sign amd obtain approval from line manager*
4 *Pass to Chief Exec or Chairman for authorisation and payment*
5 *Business mileage can be claimed at 45p per mile*

Signed: _____

Authorised: _____

Payment details: _____

11 Appendix 4 – Health and Safety

11.1 Home Working Risk Assessment Template

Use the following simple risk form to assess how safe your home working space is. Take a look at the risks in the first column, answer 'yes' or 'no' as applicable and then make a note of what needs to be done to reduce or remove the risk if necessary.

Desk Area

Risk	Yes/No	Action Required
Do you have adequate space to work comfortably?		
Is there enough space underneath your desk to stretch your legs?		
Are there trailing electrical cables around your working area that need to be tied up?		
Is your working area warm, well-lit and well-ventilated?		
Do you need a desk lamp to improve lighting?		
Is your working area clutter free so that you can focus easily on the task?		

Display Screens Set-Up

Risk	Yes/No	Action Required
Is your desk chair set up correctly? Is your lower back supported, are there armrests and are your feet flat on the floor?		
Do you have enough surface space on your desk to work comfortably?		
Are your keyboard and mouse clean and within easy reach, without having to stretch?		
Is your display screen clean and positioned so there is no glare from a window or light?		
Is your display screen level with your eyes so it doesn't cause discomfort to your neck or head?		
Can you easily reach everything that you need without twisting and straining your upper body?		

Slips, Trip and Falls

Risk	Yes/No	Action Required
Are floor coverings, such as carpets and rugs, secure?		
Do you frequently carry hot drinks and food upstairs/downstairs and risk tripping?		
Are stairways and corridors clear of trip hazards?		
Is the floor area around your desk clear of boxes, papers and wires		

Lone Working

Risk	Yes/No	Action Required
Do you know the name and number of a manager or supervisor who you can get in touch with easily?		
Do you have a system for regularly 'checking in' with your employer if you are not visibly online each day?		
Is your home kept secure whilst you're working there?		
Are important files and laptops kept locked away securely when not in use?		

Fire and Electrical Safety

Risk	Yes/No	Action Required
Are smoke detectors working and checked regularly, e.g. every month?		
Do you regularly dispose of waste, including papers, to prevent a build up of fire 'fuel'?		
Does any electrical equipment spark or show signs of burns?		
Do any wires look damaged or frayed?		
Do you regularly inspect your electrical equipment to check for signs of wear and tear?		
Do you switch off equipment when not in use?		
Do you have emergency arrangements in place in case of fire?		

Stress and Welfare

Risk	Yes/No	Action Required
Do you take regular breaks away from your workstation?		
Do you carry out regularly stretches at your desk to avoid stiff or sore muscles?		
Do you sit with a good posture or are you hunched over the desk?		
Do you have easy access to first aid equipment if required?		
If you regularly use a computer, do you have your eyes tested every year?		
Are heavy items stored on lower shelves to avoid the need for lowering them?		
Do you know how to correctly pick up, carry and lower heavy items?		

12 Appendix 5 - Data Protection

12.1 Statement for staff

As a member of staff, you are required to comply with this policy under your employment or worker contract. If you find that you have accidentally breached the policy it is important that you contact our Data Protection Officer immediately so that the impact of the breaches can be assessed. Anyone who breaches the data protection policy may be subject to disciplinary action, particularly in the following circumstances:

- There is a big gap between the person's practice and what this policy requires;
- Data subjects have been placed in significant risk of suffering damage and/or distress;
- There is a data security breach; or
- The person has breached the policy intentionally, recklessly, for personal benefit or in concert with others.

If you are appointed by us as a data processor you are required to comply with this policy under your contract with us. Any breach of the policy will be taken seriously and could lead to contract enforcement action or termination of the contract. Data processors have direct obligations under the UK GDPR, primarily to only process data on instructions from the controller (us) and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved.

As a data subject, we will use your personal information in accordance with this policy.

If you are unsure about whether anything you propose to do might breach this policy you must speak first with the Data Protection Officer.

12.2 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:

Mr David Sheldon

South Eastern Baptist Association,
17 Cherry Close, Burgess Hill, RH15 9PR

Tel: 01444 233431

Email: dataprotection@seba-baptist.org.uk

12.2.1 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.

12.2.2 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.

12.2.3 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.

12.2.4 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.

12.2.5 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.

12.2.6 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.

12.2.7 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.

12.2.8 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.

12.3 Schedule 2 – Appropriate Policy Document

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", "the Association") is an Asscoiation of approximately 150 churches across the South East of England

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 Association 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 must therefore have regard to this policy when carrying out sensitive processing on behalf of the Association.

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 Association 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.
- The Association 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 and the privacy statements on our website (www.baptist.org.uk/privacy) 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 Association 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 Support Services Team Leader and provides a legal update report to the charity trustees of the Association three times a year. Data protection training is provided by the DPO for all new staff and an annual update on data protection is provided in an all-staff meeting, to ensure that all colleagues are familiar with SEBA's data protection policies and procedures. Particular attention is given to the processing by the Ministries and Safeguarding Teams, who may be required to process special category and criminal offence data. The DPO reviews the Data Protection Impact Assessments for these teams with their Team Leaders annually. Each of the Regional Associations and Colleges have an appointed DPO and specialist training is made available to them.
- 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, details of which can be found at www.baptist.org.uk/privacy.

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 Ministries and Safeguarding Teams 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 the Association;
- A child or individual in membership with or associated with a Baptist church or organisation in membership with the Association;
- 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
- Churches – usually ministers, church officers, workers or volunteers, most commonly the minister or church's Designated Person for Safeguarding
- Regional Associations – including specialist advisers providing safeguarding advice on a voluntary basis
- Baptist Colleges
- Other BUGB Specialist Teams
- Police, Social Services or the Local Authority Designated Officer for safeguarding
- Other employing bodies e.g. hospitals or the armed forces
- Other denominational safeguarding teams at both local and national level, including the Baptist Union of Scotland and the Baptist Union of Wales

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 Privacy Notices for the Ministries and Safeguarding Teams are available on the BUGB website at www.baptist.org.uk/privacy. Both Privacy Notices set out the legal bases for our processing of special category and criminal offence data by reference to 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 the Association, 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 the Association 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 Association 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.

The Association 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. The Association discharges these functions by custom, practice and with the consensus of Baptist 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.

The Association may 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).

The Association 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.

The Association may seek to rely on this condition if it is required 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.

The Association 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.

Who we share your personal data with

We are required to share your data with third parties where we have a legal obligation to do so. We may also share information with our partner organisations with whom we have a Data Sharing Agreement, as set out in our Privacy Notices available here: www.baptist.org.uk/privacy.

The persons/organisations we may share your special category and criminal offence data with are:

- Our employees, contractors and volunteers, including the Ministerial Recognition Committee, on a need-to-know basis;
- Employees and volunteers working for one of our partner organisations with whom we have a Data-Sharing Agreement. Please see the current list of partner organisations at www.baptist.org.uk/privacy
- Churches and other appointing or employing bodies as appropriate
- The Free Churches Group
- The Baptist Ministers Fellowship
- Psalms & Hymns Trust
- The United Board
- Counsellors, professional supervisors and risk assessment consultants
- The Police and Social Services, Local Authority Designated Officers and other statutory agencies
- The Disclosure and Barring Service and our DBS Checking Company
- Other denominations, including their Safeguarding Officers.

Before sharing information with any of the above persons or organisations, careful consideration is given to the rights and freedoms of the data subject against what is needed to be shared to achieve our overarching goal of safeguarding children, young people and adults at risk from harm within our member churches and to support and promote exemplary ministry associated with the BUGB. Special category and criminal offence data is only disclosed where it is reasonably necessary to do so and a record of any disclosure to third parties is kept on a spreadsheet on the Ministries drive to enable us to identify when and why disclosures were made with details of the full disclosure on the Ministries Information Exchange "MIX" for the Ministries Team, and on the Case Information Spreadsheet for the Safeguarding Team.

Automated decision making

Currently, SEBA undertakes no automated decision making in relation to your personal data.

How we keep your data secure and how long we keep it for

The Association deploys a wide range of technical and organisational measures to protect the personal data it holds and processes. Controls include but are not limited to:

- Mandatory annual data protection training for all staff and part of the induction for new staff
- Mandatory 'Computer Security in the Workplace' training for all staff and part of the induction for new staff
- Acceptable use of IT equipment and systems defined in the IT General Policy provided to all users of SEBA systems
- Strong defences of the SEBA core IT system (e.g. Firewalls, Malware Detection & Defence)
- Encryption of data both at rest and in transit across dedicated SEBA networks where appropriate and the use of password protected documents when sharing data.
- Where needed, appropriate redaction takes place before witness statements, case notes or investigation reports are shared. Where this is not practical, those serving on decision-making panels are required to sign confidentiality agreements and to return all documents after the panel has reached its conclusion. A tracking system is in place to make sure that this takes place on each occasion.

- Deployment of Information Security Tools (e.g. Data Loss Prevention, Mobile Device Management, Secure External Email)
- Robust procedures for the reporting of any data or potential data breaches

These measures are under constant review by SEBA.

SEBA has a Data Retention Schedule which lists the data we hold and how long we hold it for. To find out how long we keep your data for please see our Data Retention Schedule.

Your rights in relation to the data we hold

Data protection legislation provides you with a number of rights relating to your personal data, including your special category and criminal conviction etc data. These rights are subject to some specific exemptions. Your rights may include:

- the right to access your data
- the right to have your data corrected if it is wrong or incomplete
- the right to request restrictions to the processing of your data
- the right to object to your data being processed
- the right to have your data erased
- the right to be informed about how your data is processed
- rights relating to automated decision making and data portability

You should keep us informed of any changes to your information so that we can be confident that the data we hold about you is accurate. To understand more about these rights and how to exercise them please see our Privacy Notice www.baptist.org.uk/privacy and the Information Commissioner's Office website: https://ico.org.uk/.

Data Protection Officer

Our Legal Services Manager (Caroline Sanderson) is our **Data Protection Officer** and she is the person responsible for matters relating to the protection of personal data. She can be contacted at the address below or by email (dataprotection@baptist.org.uk) or phone 01235 517700.

Your right to complain to the Information Commissioner

If you are unhappy with any aspect of the way in which we have processed your personal data, you have the right to make a complaint to the Information Commissioner's Office:

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
www.ico.org.uk
Tel: 0303 123 1113
casework@ico.org.uk

Feedback or complaints about the Association or staff

If you want to give us feedback or make a complaint about the Association or its staff in relation to the handling of your personal data, please contact

Mr David Sheldon
South Eastern Baptist Association
17 Cherry Close, Burgess Hill, RH15 9PR

Tel: 01444 233431
Email: dataprotection@seba-baptist.org.uk

Review of this policy

This policy will be regularly reviewed and may be subject to revision. Please visit our website to check for any updates.

12.4 Data Retention Schedule

Employment/HR	All information relating to recruitment, selection and development whilst in post	6 years after post-holder has left your employment	Limitation Act 1980	Destroy
	Information on any disciplinary or grievance matter that is still 'live' on the individual's personnel file, including information on any penalty or warning imposed	6 years after post-holder has left your employment	Limitation Act 1980	Destroy
	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 your employment	Limitation Act 1980	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 under Safeguarding below)	Requirements of the Independent Inquiry into Child Sexual Abuse (IICSA)	Not applicable
	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	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

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 church)	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	Good practice	Archive on line
	Payroll records including correspondence with HMRC	See Employment/HR above	See Employment/HR above	See Employment/HR above

General	Correspondence (including emails)	Unless this relates to any other category of data listed here (e.g. finance, employment, safeguarding etc) correspondence should be kept for as long as is relevant. Workers should review all retained correspondence annually and destroy any which is no longer relevant.

Governance	Trustee Meeting Minutes	10 years from the date of the meeting [(3)]	Good practice	Archive online
	Other formal minutes	5 years from the date of the meeting	Good practice	Destroy
	Certificate of incorporation	Permanently	Companies Act 2006, s 15 (CA 2006)	Not applicable

	New certificate of incorporation to reflect change of company name	Permanently	CA 2006, s 80	Not applicable
	Memorandum & articles of association (signed original)	Permanently	CA 2006, ss 8 anD 18	Not applicable
	Accounting records	6 years from the date on which the record was made (private companies)	CA 2006, ss 386 AND 388	Destroy
	Records of all proceedings at Directors' meetings, including: —Board minutes —written resolutions of the Board —register of sealed documents	10 years from the date of the meeting	CA 2006, S 248 and historical interest	Archive online
	Minutes of all proceedings of general meetings	10 years from the date of the meeting then archive	CA 2006, S 355	Archive online
	Copies of all members' resolutions passed outside general meetings	10 years from the date of the resolution	CA 2006, S 355	Archive online
	Reports and accounts required by HMRC (if applicable)	6 years	Value Added Tax Act 1994 (VATA 1994), SCH 11 S 6	Destroy
	Register of Directors and their residential addresses	Indefinitely for the register itself	CA 2006, s 162	NOT APPLICABLE
	Register of Secretaries	Indefinitely for the register itself	CA 2006, s 275	Not applicable
	Register of disclosed interests	Indefinitely for the register itself	CA 2006, ss 793, 808, 816 and 817	Not applicable
	Register of members	An old entry may be removed from the register if more than six years have elapsed since the entry was made	CA 2006, ss 113 and 121	Usually not applicable

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 Occurrences Regulations 2013	Destroy
	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
	Product liability policies	Permanently	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
	Professional Indemnity Insurance policies	Permanently	Commercial practice	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

Ministerial	Special category and criminal convictions etc ("criminal offence data") relating to accredited ministers, non-accredited ministers and those who are nationally recognised for ministry	75 years from the date of retirement. For a minister who ends his or her accreditation or recognised status with the Union prior to retirement, 75 years from the date accreditation/recognition ceases.	To safeguard against any risks posed to others under GDPR where the processing is necessary for the purposes of the legitimate interests of the Association, except where such interests are overridden by the interests or fundamental	Destroy after 75 years.

			rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Where it fulfils one of the substantial public interest conditions from Schedule 1, Part 2 of the Data Protection Act 2018, in particular, Conditions 10, 11, 12, 18 and 19 and Condition 31 from Schedule 1, Part 3 of the Data Protection Act 2018. See the Association Data Protection policy and Appropriate Policy Document.	
	Special category or criminal offence data relating to "low-level concerns" i.e. where there are concerns in relation to a data subject that are not (or not yet) sufficiently serious to raise with the police or are not subject to a disciplinary process. The retention of low-level concern data enables patterns of repeated behaviour which may indicate that there is an underlying serious safeguarding concern to be identified and assessed, to mitigate the risk of individuals committing criminal offences (including of a sexual nature)	To be reviewed after 10 years to determine whether data should be retained in line with other ministerial records for 75 years or destroyed	Conditions 10, 11, 12, 18, 19 and 31 of Schedule 1 Data Protection Act 2018 as set out above.	Destroy

	and to assess individuals' ongoing suitability for ministry, including by reference to risks they may pose to others.			

Property	Title Deeds for property owned by SEBA	Permanently or until property is disposed of	Limitation Act 1980	Keep copy for 6 years after property has been disposed of
	Files relating to property sales and purchases	6 years from date of completion	Limitation Act 1980	Destroy
	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	Records of safeguarding incidents, allegations or concerns	75 years after last contact with the individual concerned	Good practice	Destroy
	Records that relate to safeguarding concerns/allegations about church workers (paid or voluntary)	75 years after employment/role ceases	Good practice	Destroy
	Risk assessments / safeguarding contracts concerning known or alleged offenders	75 years after last contact with the individual concerned	Good practice	Destroy
	Registers / records of events or activities	3 years after the event	Good practice	Destroy
	Parent / carer consent forms	3 years after the form has been completed	Good practice	Destroy
	First Aid / accident forms	3 years after the form has been completed	Good practice	Destroy

	Health and safety risk assessment	3 years after the risk assessment has been completed	Good practice	Destroy
	Minister personnel records where there are safeguarding allegations / investigations, regardless of the findings	75 years from the date of the minister's death	Good practice	Destroy
	Personnel records relating to workers whose role involves contact with children and adults at risk	75 years after employment/role ceases	Good practice	Destroy
	Record of a Disclosure and Barring Service (DBS) check being undertaken for a church worker (paid or voluntary)	75 years after employment/role ceases	Good practice	Destroy
	Record of a minister's DBS check history	75 years from the date of the minister's death	Good practice	Destroy
	Record of a church worker's (paid or voluntary) disciplinary procedure relating to safeguarding allegations / offences	75 years after employment/role ceases	Good practice	Destroy
	Record of a minister's disciplinary procedure relating to safeguarding allegations / offences	75 years from the date of the minister's death	Good practice	Destroy