Data Policy Suite

Privacy Policy

Data Protection Policy

Data Retention Policy

DOCUMENT TITLE: AMIE DATA POLICY SUITE		
OWNER: AMIE STANDING COMMITTEE		
APPROVING BODY: STANDING COMMITTEE		DATE OF APPROVAL: NOVEMBER 2021
VERSION: 1.0		NEXT REVIEW DATE: NOVEMBER 2022
SUPERCEDES: N/A	PREVIOUS REVIEW DATE:	MONITORING REVIEW:
PUBLIC USE: YES	STANDING COMMITTEE USE: YES	OTHER USE: REGULATORS
CHARITY REGISTRATION NUMBER: 1158679		COMPANY REGISTRATION NUMBER: 9042552

Our Data Protection Officer at the time off issuing these policies is Jan Draper. Any questions about these policies should be addressed to them.

Privacy Policy

Your Personal Data- What is it?

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

Who are we?

The Anglican Mission in England (AMiE) is the data controller (contact details below). This means it decides how your personal data is processed and for what purposes.

How do we process your personal data?

The Anglican Mission in England complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

We use your personal data for the following purposes:

- To enable us to provide a voluntary service for the benefit of the public in a particular geographical area as specified in our constitution;
- To administer partnership records;
- To fundraise and promote the interests of the charity;
- To manage our employees and volunteers;
- To maintain our own accounts and records (including the processing of gift aid applications);
- To inform you of news, events, activities and services running at The Anglican Mission in England or other Christian events.

What is the legal basis for processing your personal data?

- Explicit consent of the data subject so that we can keep you informed about news, events, activities and services and process your gift aid donations and keep you informed about diocesan events.
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided:
    - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
    - there is no disclosure to a third party without consent.

Sharing your personal data

Your personal data will be treated as strictly confidential and will only be shared with other members of the church in order to carry out a service to other church members or for purposes connected with the church. We will only share your data with third parties outside of the church with your consent.

How long do we keep your personal data?

We keep data for no longer than is necessary for the purposes for which it **is** being processed. Specifically, we retain partnership data while it is still current; gift aid declarations and associated paperwork for up to 7 years after the tax year to which they relate.

Your rights and your personal data

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

i) The right to request a copy of your personal data which AMiE holds about you;
ii) The right to request that AMiE corrects any personal data if it is found to be inaccurate or out of date;
iii) The right to request your personal data is erased where it is no longer necessary for AMiE to retain such data;
iv) The right to withdraw your consent to the processing at any time
v) The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability);
vi) The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
vii) The right to object to the processing of personal data.

Further Processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Contact Details

To exercise all relevant rights, submit queries or complaints, in the first instance, please email: info@anglicanmissioninengland.org

Data Protection Policy

Preface

The data protection policy is an internal AMiE document, written so that The Anglican Mission in England can establish a company-wide data protection policy available to all employees, trustees and voluntary workers and everyone in any leadership position can understand the importance and significance of data protection security and why they must be acquainted with the principles laid out therein. The overall aim is to demonstrate GDPR compliance.

Any organisation that collects data will be required to uphold GDPR requirements for that data, according to GDPR Article 24:
"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

GDPR Article 39 sets out the tasks of the data protection officer.

1. The data protection officer shall have at least the following tasks:
    i) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
    ii) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
    iii) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
    iv) to cooperate with the supervisory authority;
    v) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

This policy demonstrates that AMiE will document and establish that AMiE processes data in compliance with the GDPR according to the purposes of AMiE, its scope, context of AMiE data processing activities.

Introduction

The Anglican Mission in England adopts the data protection rights that are relevant to the jurisdiction of country in which it is operating.

For the UK the following applies:
On 25th May 2018 the General Data Protection Regulation (GDPR) came into force, replacing the existing Data Protection Act. The main principles are similar, but there is an increased need to be able to show compliance and accountability. GDPR gives individuals more rights and protection in how their personal data is used by organisations.

To ensure compliance:

i) A record should be kept of what actions are being taken in AMiE to comply with the GDPR, for examples logs of meetings to discuss GDPR, keeping records of attendance.
ii) Conduct a data audit that identifies what information is held, where, why and how long it will be kept for and with whom the data may be shared.
iii) Ensure that any sensitive data information is securely locked away in filing cabinets, password protected computers etc.
iv) Have a Privacy Policy available on the AMiE website and require AMiE Ministers to regularly update their congregations.
v) Have due processes ready to act on if there are any breaches of data.
vi) Keep any relevant information that is held up to date. If details are out of date remove them.

Policy

Our Data Protection Officer will be able to answer questions about this policy and should be addressed to them. This policy should also be read in conjunction with the Privacy Policy.

Normal photos are actually even sensitive data, as they reveal gender, racial and even ethnic origin, can contain geolocation and time information etc. Civil proceeding can be taken if a person is filmed without consent, and privacy laws exist to protect a person where they can expect privacy.

As photographs **can constitute personal data under the GDPR**, this means we must be able to quickly and easily remove all images where the individual can be identified. Failure to do so means failure to comply with the GDPR and Article 17, and the fines for breaching compliance can be seriously damaging.

Overview

We gather and use information or 'data' about you as part of our activities and this policy sets out the things we must tell you about data protection.

We take the security and privacy of your data seriously and are required to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security.

This policy applies to current and former employees and volunteers who are 'data subjects' for the purposes of this policy. This policy should be read alongside your employment contract (if an employee) and any other notice we issue from time to time in relation to data usage.

The Anglican Mission in England (AMiE) is a 'data controller' for the purposes of your personal data. This means it decides how your personal data is processed and for what purposes, as governed by the 2018 Act and the GDPR.

Throughout this policy the term 'you' refers to you as a data subject. The term 'we' refers to us as data controller.

This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing, or storing personal data while working for, or on behalf of, AMiE.

It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the 2018 Act and the GDPR take precedent.

Data protection principles

Personal data must be processed in accordance with the following six lawful bases as data protection principles as set out in Article 5
It must be:

i) processed in a lawful, fair and transparent manner;
ii) collected and processed only for specified, explicit and legitimate purposes;
iii) adequate, relevant and limited to what is necessary for the purposes for which it is processed;
iv) accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
v) kept for no longer than is necessary for the purposes for which it is processed;
vi) be processed securely and confidentially.

As data controller, we are responsible for ensuring and demonstrating compliance with these principles.

Definition of personal pata

Data includes genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which might come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper, or in/on other materials.

This personal data might be provided to us by you, or by someone else (such as a former employer, your doctor), or it could be created by us. It could be provided or created during the recruitment process or during the employment contract or after it has ended. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- Your contact details and date of birth
- The contact details for your emergency contacts
- Your gender
- Your marital status and family details
- Information about your employment contract including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement
- Your bank details and information in relation to your tax status including your National Insurance number
- Your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us
- Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings)
- Information relating to your performance and behaviour at work
- Training records
- Electronic information in relation to your use of IT systems/swipe cards/telephone systems
- Your images (whether captured on CCTV, by photograph or video)
- Any other category of personal data which we may notify you of from time to time.

Special categories of personal data

'Special categories of personal data' are types of personal data consisting of information about:

- your racial or ethnic origin
- your political opinions
- your religious or philosophical beliefs
- your genetic or biometric data
- your health
- your sexual orientation.

We may hold and use any of these special categories of your personal data in accordance with the law.

Definition of data processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storing
- adaption or alteration
- retrieval, consultation or use
- disclosure by transmission, dissemination or otherwise making available
- alignment or combination
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

Processing of personal data

We will process your personal data (including special categories of personal data) in line with our obligations under the 2018 Act.

We will use your personal data:

- for performing the employment contract (or contract for services) between us
- for complying with any legal obligation
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else).

However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights below (on page 11).

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to give us certain personal data, we may not be able to carry out some parts of the contract between us. For example, if we do not have your bank account details, we may not be able to pay you. It might also prevent us from complying with certain legal obligations and duties, such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may have.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment/engagement and even following termination of your employment/engagement. For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including, where relevant, its termination;
- to train you and review your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of AMiE, you, our other staff, customers and others;

- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- to pay tax and National Insurance;
- to provide a reference upon request from another employer;
- to monitor compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- for the prevention and detection of fraud or other criminal offences;
- to defend AMiE in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- and for any other reason which we may notify you of from time to time.

**asterisks indicate that consent to process data may not be needed if processing is for one of the specified purposes below.*

We will only process special categories of your personal data (see 'Special Categories of Personal Data' section above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we ask for your consent to process a special category of personal data, then we will explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Data Protection Officer.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes:

i) where it is necessary for carrying out rights and obligations under employment law;
ii) where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
iii) where you have made the data public;
iv) where processing is necessary for the establishment, exercise or defence of legal claims;
v) where processing is necessary for the purposes of occupational health or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes in 'Examples of when we might process your personal data' which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under

employment law including to make reasonable adjustments and to look after your health and safety

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data

Sometimes we might share your personal data with others to carry out our obligations under our contract with you or for our legitimate interests.

We require those people and companies to keep your personal data confidential and secure, and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area. If this changes, we will tell you. We will also explain the protections that are in place to protect the security of your data.

How should you process personal data for the Anglican Mission in England?

Everyone who works for, or on behalf of, AMiE has some responsibility for ensuring data is collected, stored, and handled appropriately, in line with this and other relevant policies.

You should only access personal data covered by this policy if you need it for the work you do for or on behalf of AMiE and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

Your computer and any other devices on which you store data must be password protected.

You should use strong passwords.

You should lock your computer screens when not at your desk.

Personal data should be encrypted before being transferred electronically to authorised external contacts.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.

You should lock drawers and filing cabinets. Do not leave paper that contains personal data lying about.

You should not take personal data away from your place of work without authorisation from your line manager or Data Protection Officer.

Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from the Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you under the Disciplinary Policy.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under the Disciplinary Policy and you could be dismissed.

How to deal with data breaches

If this policy is followed, we should not have any data breaches. But, if a breach of personal data occurs (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours, where feasible.

If you are aware of a data breach you must contact the Data Protection Officer immediately and keep any evidence you have in relation to the breach.

Subject access requests (SAR)

Data subjects can make a 'subject access request' to find out what information we hold about them. This request must be made in writing. If you, in the course of your work for AMiE, receive a SAR you should forward it immediately to the Data Protection Officer who will coordinate a response.

If you wish to make a SAR in relation to your own personal data, you should write to the Data Protection Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by up to two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request.

Your Data Subject Rights

You have the right to information about what personal data we process, how and on what basis, as set out in this policy.

You have the right to access your own personal data by way of a SAR (see above).

You can correct any inaccuracies in your personal data by contacting the Data Protection Officer.

You have the right to request that we erase your personal data where we were not entitled under law to process it, or where it is no longer necessary to process the data for the purpose for which it was collected. You can request erasure by contacting the Data Protection Officer.

During the process of requesting that your personal data is corrected or erased, or while you are contesting the lawfulness of our processing, you can ask for the data to be used in a restricted way only. To do this, contact the Data Protection Officer.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and, with some exceptions, to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.
You have the right to be notified of a data security breach concerning your personal data where that breach is likely to result in a high risk of adversely affecting your rights and freedoms.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has more information on your rights and our obligations.

Data Retention Policy

Introduction

The Anglican Mission in England Data Retention Policy is a set of guidelines that helps AMiE to keep track of how long information must be kept and how to dispose of information when it is no longer needed.

The policy outlines the purpose for processing personal data to ensure that AMiE has documents proof that justifies data retention and disposal periods.

The AMiE Trustees consider that data retention periods are essential and to limit damage that data breaches can cause, the regulators mandated that EU-based organisations must retain personal data only if there is a legitimate reason for keeping it.

The UK GDPR contains explicit provisions about documenting our processing activities.

Records must be maintained on several things such as processing purposes, data sharing and retention.

Records, documentation, will be kept in writing, electronically so that we can add, remove and amend information easily, and reflect the current processing activities.

As a designated 'small organisation' The Anglican Mission in England will only need to document processing activities that:

i) are not occasional; or
ii) could result in a risk to the rights and freedoms of individuals; or
iii) involve the processing of special categories of data or criminal and offence data.

Under Article 30 of the GDPR we will document the following information:

i) The name and contact details of The Anglican Mission in England (and where applicable, of other controllers, AMiE representative and the AMiE data protection officer).
ii) The purposes of our processing.
iii) A description of the categories of individuals and categories of personal data.
iv) The categories of recipients of personal data.
v) Details of our transfers to third countries including documenting the transfer mechanism safeguards in place.
vi) Retention schedules.
vii) A description of your technical and organisational security measures.

The Anglican Mission in England will comply with the UK GDPR and the UK's Data Protection Act 2018. Documentation may include:

i) information required for privacy notices, such as:
    - the lawful basis for the processing

- the legitimate interests for the processing
- individuals' rights
- the existence of automated decision-making, including profiling
- the source of the personal data;

ii) records of consent;

iii) controller-processor contracts;

iv) the location of personal data;

v) Data Protection Impact Assessment reports;

vi) records of personal data breaches;

vii) information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018, covering:

- the condition for processing in the Data Protection Act;
- the lawful basis for the processing in the UK GDPR; and
- your retention and erasure policy document.

This policy will be reviewed regularly to address such issues as retention, security and data sharing.

Documentation

The Anglican Mission in England will regularly review what personal data we hold and where it is by reviewing policies, procedures, contracts and agreements

All documentation of findings will be kept in writing and information will be documented in a granular and meaningful way; all policies, procedures, contracts and agreements will be regularly reviewed.

Processes will be enabled through the use of the linked ICO templates:

Documentation template for controllers
For organisations
File (31.22K)

Documentation template for processors
For organisations
File (19.48K)

Further reading:
Relevant provisions in the UK GDPR – See Article 30 and Recital 82
External link

Relevant provisions in the Data Protection Act 2018 – See Schedule 1
External link

Roles and Responsibilities

Trustees and those involved with safeguarding will adopt the retention and disposal guidance at Appendix 1 of this policy and strive to keep records up to date.

The Anglican Mission in England Data Protection officer will advise about any uncertainty about retention periods.

Retention and Disposal

Advice can be obtained from The Anglican Mission in England Data Protection Officer if there is uncertainty about retention periods.

GDPR sets no rules on storage limitation. The Anglican Mission in England sets its own deadlines as it sees fit for purpose based on the purpose for processing the data, and any regulatory or legal requirements for retaining it. *(See Appendix 1)*

Personal data may be kept for longer if it is in the public interest so to do for example for archiving, scientific or historical research, or statistical purposes.

Data will not be held for longer than it is needed and shouldn't be kept 'just in case' The Anglican Mission in England might have a need for it in the future. The data held by The Anglican Mission in England will be periodically reviewed. However, if one of The Anglican Mission in England's purposes still applies, The Anglican Mission in England will continue to store data.

The Anglican Mission in England will comply with individuals' requests for erasure under 'the right to be forgotten.'

Consideration of legal and regulatory requirements to retain data will be made, such as when the data is subject to tax or audits, or to comply with defined standards, there will be data retention guidelines that must be followed.

Personal data will be either erased (deleted), or anonymised.

Note: *If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. If personal data is still being processed data can only be stored offline (rather than deleted) if there is still justification for holding it. The Anglican Mission in England will respond to subject access requests for personal data stored offline, and will comply with all the other principles and rights.*

The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data. The key issue The Anglican Mission in England will ensure is that the data is put beyond use. If it is appropriate to delete personal data from a live system, data will be also deleted from any back-up of the information on that system.

Data Sharing

When any data shared with other organisations is no longer needed there will be an agreement between both parties as to what happens to that data. It will either be returned to the other organisation who supplied the data initially, without a copy being kept by The Anglican Mission in England, or, all copies will be deleted.

Retention periods for organisations involved in information sharing may differ for good reasons. However, if data is held for the purposes of the original data-sharing initiative and it is no longer needed for that initiative, then all organisations with copies of the information should delete it.

Appendix 1

Illustrative Data Retention Schedule

This Schedule is provided as a guide to common types of documents but is not exhaustive.

NOTE: There may be an historic interest in The Anglican Mission in England's records.

Avoid retaining information if there is no reason for doing so. Consult with the Data Protection Officer if you are unsure.

Retention Period

Record	Time Period
Minutes of meetings	6 years
Trustee meetings	50 years
Pre-employment enquiries/applications/notes/letters/references	6 months after completion of recruitment (unless data to be retained for a future similar opportunity, in which case 1 year)
Safeguarding Service confirmation of advice, emails, letters	100 years
Confidentiality Agreements	100 years
Covenants of Responsibility (managing those who pose a risk)	100 years
Safeguarding Service Risk Assessments	100 years
Complaints concerning people	100 years
Congregational Register	100 years
Safeguarding Audit for The Anglican Mission in England and the Congregations	100 years
Transfer Forms	100 years
Employee records including: contracts, time records etc.	Duration of employment + 6 years
Volunteer records	Duration of placement + 6 years
Databases for mailing lists/distribution	Reviewed annually, delete out of date information
Miscellaneous contact information	Delete once there is no longer a requirement to hold such information
Arranged accommodation/placements (e.g. overseas visitors)	3 years following end of event/placement
Documents relating to litigation or potential litigation	Until matter is concluded plus 6 years
Hazardous material exposures	30 years

Injury and Illness Incident Reports (RIDDOR)	5 years
Pension plans and retirement records	Permanent
Salary schedules; ranges for each job description	2 years
Payroll Records	Minimum, 6 years. No maximum
Contracts	6 years following expiration
Construction documents	Permanent
Fixed Asset Records	Permanent
Application for charitable and/or tax-exempt status	Permanent
Sales and purchase records	5 years
Resolutions	Permanent
Audit and review workpapers	5 years from the end of the period in which the audit or review was concluded
OSCR/Charity Commission filings	5 years from date of filing
Records of financial donations	6 years
Accounts Payable and Receivables ledgers and schedules	6 years
Annual audit reports and financial statements	Permanent
Annual plans and budgets	2 years
Bank statements, cancelled cheques, deposit slips	Minimum of 6 years
Business expense records	6 years
Cash receipts	3 years
Cheque registers	Permanent
Electronic fund transfer documents	6 years
Employee expense reports	6 years
General ledgers	Permanent
Journal entries	6 years
Invoices	6 years
Petty cash vouchers	3 years
Tax records	Minimum 6 years
Filings of fees paid to professionals	6 years
Environmental studies	Permanent
Insurance claims/applications	Permanent
Insurance disbursements and denials	Permanent
Insurance contracts and policies (Directors and Officers, General Permanent Liability, Property, Workers' Compensation)	Permanent
Leases	6 years after expiration
Real estate documents (including loan and mortgage contracts, title deeds)	Permanent
Warranties	Duration of warranty + 6 years
Records relating to potential, or actual, legal proceedings	Conclusion of any tribunal or litigation proceedings + 6 years

Appendix 2

General guidance for documents NOT included in the retention schedule.

On-going business use is subjective, but generally refers to documents still required for on-going projects, or documents that may still need to be referred to for on-going activities.

Example of process: