



Church of England Information Sharing Framework

VERSION 1.0

JANUARY 2022

Contents

Approval and review	3
Version Control.....	3
1. Summary Sheet.....	4
2. Introduction	5
3. Purpose	7
4. Scope.....	8
5. Principles	8
6. Responsibilities	9
7. Lead Signatory.....	10
8. Partners	10
9. Nominated Individuals	11
10. Information Sharing Agreements (ISAs)	11
11. Other Data Sharing Agreements.....	11
12. Data Protection Impact Assessment (DPIA)	11
13. Sharing and disclosing data	12
14. Shared or integrated systems	12
15. Ad-hoc Information Sharing	13
16. One-way disclosure of information.....	14
17. Authorisation	14
18. Requesting data.....	14
19. Decision not to share	14
20. Use of Shared Data	14
21. Third Parties	14
22. International transfers	15
23. Data handling and management.....	15
24. Transfer methods.....	16
25. Subject Right Requests and complaints	17
26. Appropriate Policy Document	17
27. Training and awareness.....	17
28. Breach Management.....	18
29. Dispute Resolution.....	19
30. Processes	19

31.	Framework Termination	20
32.	Indemnity	20
	Appendix A - Definitions (alphabetic).....	21
	Appendix B - Ad-hoc Data Sharing Request Form.....	24
	Appendix C - Breach Reporting Form.....	26
	Appendix D - Signatories and Nominated Individuals	28

Approval and review

Approved by	Chief Operating Officer and Senior Risk Owner, Church of England Central Services
Framework owner	Director of Information Management, Church of England Central Services
Framework author	Information Governance Officer, Church of England Central Services; Legal Office, Church of England Central Services; Stephens Scown LLP
Date	15 March 2022
Review date	April 2026

Version Control

Version No	Revision Date	Amended by	Summary of Changes
0.1	April 2018	Information Governance Officer	Finalisation of draft from Inform-Consult.
0.2	June 2019	Information Governance Officer	Amendment of Inform-Consult draft for consultation.
0.3	June 2021	Information Governance Officer	Incorporated Framework, Policy and Framework into single document; document updated to meet new ICO statutory guidance.
0.4	August 2021	Stephens Scown LLP	External review, revision and consolidation.
0.5	September 2021	Information Governance Officer	Formatting; addition of appendices
1.0	December 2021	Information Governance Officer; NCIs Legal office	Amendments following consultation and internal review. Approved.

Foreword

Recent changes to data protection legislation have created the most robust laws in this area the UK has ever seen. The principles outlined within the law give people greater rights over their personal data and impose greater responsibilities on organisations, with much greater liabilities for those who disregard such rights. In order to comply with the law, and to be able to share personal data where and when we need, the Church of England needs to adopt a clear Framework for data sharing.

Why does the Church need an Information Sharing Framework?

In the course of its activities, the Church collectively process a significant amount of personal data and special category data (personal data that holds a greater level of justification and expectation in its use such as information about religious belief). All parts of the Church must of course comply with the law when processing such data.

Various parts of the Church will inherently need to share personal data with one another to perform its functions effectively and in particular their safeguarding functions – however, due to fact that the church is many separate legal entities not one organisation, such activities are likely to be considered ‘transfers’ of personal data under data protection legislation. Therefore, there needs to be a clear and robust legal framework within which data can be shared when needed.

In addition, the IICSA report into the Anglican Church made specific recommendations to improve data sharing between not only all Church of England organisations but with the Church in Wales too.

Putting an Information Sharing Framework in place will allow us all to share the data we need to in support of our work and mission and will enable us to meet the IICSA recommendations both Churches have committed to implementing.

How does the Information Sharing Framework operate?

The Information Sharing Framework is the overarching framework governing data sharing between independent Church Bodies (known as Partners). As a member of the Framework, each Partner agrees be subject to standards set out in the Framework.

The Framework will be supplemented by Information Sharing Agreements (ISAs) which form the contractual basis for data sharing/processing between the Partners. Universal ISAs applicable to all Partners have been created for areas of high importance (for example HR and Safeguarding) where a cohesive approach is required across the Church. These universal ISAs cannot be edited or amended by the Partner independently and must be adopted in their full form. Outside of these universal ISAs, bespoke ISAs can be determined between Partners from time to time and we can provide an editable template for their assistance and use in this regard.

Any ISA provided to Partners under the framework will meet legal requirements by detailing the Partners’ role under data protection legislation, the data types being shared, the reasons for sharing such data between Partners and how the data will be shared relative to that specific purpose.

How can I be sure that this will enable me to share data?

These documents have been drawn up for just this purpose by the Church of England’s legal and data protection specialists and then been reviewed by independent data protection legal experts at Stephens Scown. The work has been overseen throughout by a project team drawn from the Church of England legal, Safeguarding, HR, and Data protection staff; and the Church in Wales. There has also been consultation at key points with representatives from the wider church including dioceses and cathedrals.

Rosie Slater-Carr
Chief Operating Officer and Lead Signatory
Church of England Central Services



1. Summary Sheet

Title	Church of England Data Sharing Framework
Framework Reference	CoEV01/I0322/R2025
Purpose	The purpose of the Framework is to facilitate the lawful sharing of Personal Data among Partners.
Lead Organisation	Church of England Central Services (ChECS)
Lead Signatory	Chief Operating Officer and Senior Risk Owner, ChECS
Partners	<ul style="list-style-type: none">• National Church institutions (NCIs)– consisting of the Archbishops’ Council, The Archbishop of Canterbury (in his corporate capacity), The Archbishop of York (in his corporate capacity), The Church Commissioners for England, The Church of England Pensions Board, The National Society for Promoting Religious Education, Church of England Central Services (ChECS),• The Church of England Central Services Trading Limited;• Diocesan Bishops, Suffragan Bishops, Area Bishops (in their corporate capacity)• Provincial Episcopal Visitors of the Church of England (where they are data controllers).• Diocesan bodies (including Diocesan Boards of Finance, Diocesan Boards of Education etc);• Cathedrals and Peculiars of the Church of England;• The Representative Body of the Church in Wales. <p>The list of Partners is provided in Appendix E as signatories to the Framework.</p>
Date Framework comes into force	1 st March 2022
Date of Framework review	February 2025
Framework owner	Chief Operating Officer and Senior Risk Owner, ChECS
Framework drawn up by	NCIs Data Protection Officer; NCIs Legal Office; Church in Wales Legal Office; Thomas Chartres-Moore, Partner at Stephens Scown LLP

2. Introduction

2.1 The Partners shall be those bodies and organisations listed from time to time in the Summary and are the parties to this Framework.

2.2 This Framework sets out the overarching arrangements for data sharing by the parties to it.

2.3 This Framework applies to the following data types:

Personal Data	Any information that relates to a Data Subject, including any information which can be used to identify a Data Subject.
Special Category Data	Specific types of Personal Data or information that require additional care being taken when processing. The categories are: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.
Criminal Offence Data	Personal data relating to criminal convictions and offences or related security measures, including criminal activity; allegations; investigations; and proceedings.
Confidential Information	Information subject to a common law duty of confidentiality. This duty does not apply to information concerning the commission of a crime or other misconduct, either in the past, or in the future, if it is in the public interest that the information should be disclosed.

2.4 For the avoidance of doubt, the Framework does not govern the sharing of any data not subject to Data Protection Legislation including but not limited to:

Deceased Individual Data	Data where the information relates only to a deceased individual. Data concerning a deceased person which may identify any other Data Subject (for example, family members of the deceased) is considered to be Personal Data as defined above.
Anonymised Data	Information that has been aggregated, or has been edited to remove all personal identifiers and no longer relates to specific individuals; has been fully anonymised to replace personal identifiers in contexts where such data cannot be linked to any Personal Data.

2.5 This Framework will be supplemented by individual Information Sharing Agreements (ISA's) that detail the Data Types being shared; the reason it is being shared and how it will be shared between the Partners (for example, in respect of safeguarding). This Framework is supported by and should be read in conjunction with the relevant ISA, together with the Information Sharing Procedure/Guidance and the Ad-hoc Data Sharing Request Form (Appendix C).

2.6 Defined terms are denoted by capitalisation and are used throughout this Framework (and may also apply to ISAs). A full list of defined terms is provided in Appendix A.

2.7 All additional documents required by this Framework are provided as Appendices to this Framework.

2.8 In this Framework and all related documents, "data sharing" means the provision of data from one or more Partners to another Partner. This can take the form of:

Systematic Data Sharing	Routine sharing of data between Partners for an agreed purpose under the ISA. Partners who wish to systematically share data must become an ISA Signatory of the relevant ISA, which sits alongside this Framework.
--------------------------------	---

Ad-Hoc Data Sharing	Any exceptional, one-off internal data sharing for purposes which are not covered by Systematic Data Sharing above.
----------------------------	---

- 2.9 Neither the Framework nor the ISAs require that all data shared must at all times be shared with all Partners; what is shared and with whom will depend on the terms of the relevant ISA and will therefore be described and agreed in each individual ISA.
- 2.10 The NCIs will manage the national Framework and ISAs and will hold an Information Sharing Register for all data sharing agreements or ISAs entered into by the NCIs in order to monitor what data is being shared, by whom and with whom and for how long, and will put in place a review process.
- 2.11 This Framework is based on the understanding that, unless specific legal constraints exist, there is a general ability to share data between the Partners insofar as this sharing is compliant with Data Protection Legislation, and where relevant, ecclesiastical law.
- 2.12 In some circumstances it is permissible to share data in accordance with a Church of England policy or by a statutory provision without the need for an ISA, by way of example only (and not limited to):
- the prevention and detection of crime (including the safeguarding of children and vulnerable adults); or
 - the apprehension or prosecution of offenders.
- 2.13 In such circumstances it will be incumbent on Partners to take the necessary steps to share information across the Church and with their advisors. It may also be necessary to share with external organisations and agencies such as local authorities, HMRC, the Charity Commission, the Information Commissioner’s Office (ICO) or law enforcement bodies. A Data Sharing Request Form may be required.
- 2.14 The Framework does not apply to the sharing of Personal Data within a Partner’s own organisation (e.g. between safeguarding and finance within the Diocesan Office), as the data controller is the same. However, the principles set out in this Framework may be applicable to such disclosure.

3. Purpose

- 3.1 Data sharing is fundamental to the ongoing operation of the Church of England and the Church in Wales. The Church of England is not a single legal entity, but a collection of many different organisations, it needs to share data across its many entities regularly and consistently and does so using this Information Sharing Framework (ISF) and Information Sharing Agreements (ISA’s). The primary priorities are to ensure that data is shared appropriately and lawfully. In the same way, data needs to be able to be shared between the institutional Church of England and the Church in Wales.
- 3.2 The purpose of the Framework is to:
- facilitate the lawful sharing of Personal Data among Partners;
 - ensure the efficient operation of the Church in delivering its mission, aims and objectives;
 - create an effective, consistent, secure and reliable mechanism for data sharing between the Partners;
 - formalise the basis for data sharing activities and ensure any inherent risks are appropriately managed; and
 - protect Partners from allegations of unlawful use of data and resulting damage/fines.

4. Scope

- 4.1 The scope of this Framework covers all data sharing by the Partners. The principles of this Framework can also be applied to organisations who actively work within or with Partners, e.g.:
- Parishes (e.g. Parochial Church Councils (PCCs));
 - Schools;
 - Charities;
 - Anglican Communion;
 - Religious Communities;
 - Local Authorities;
 - Central government;
 - Police;
 - Other external agencies and organisations.
- 4.2 The above is a non-exhaustive example of possible organisations with whom data may be shared.
- 4.3 It is up to the relevant Partner to decide with whom they need to share data and to ensure that they have a sufficient purpose and lawful basis.
- 4.4 If a Partner intends to share data with an organisation such as those listed above it is their responsibility to ensure an appropriate agreement is in place. A Partner should take legal advice in respect of entering into data or information sharing agreements with third parties.
- 4.5 This Framework does not cover data that is provided to any third party Data Processor and does not function as a data processing agreement.

5. Principles

- 5.1 All Partners will accept and abide by the following principles:
- All Partners to this Framework are committed to a collaborative approach and the Partners will work together on significant changes to and decisions about the Framework or data sharing processes.
 - This Framework is intended to provide a robust mechanism for the exchange of data to support any lawful and legitimate activities with which the Partners are involved, such as:
 - the operation and development of the institutions of the Church;
 - fundraising for charitable projects;
 - working with charities, local authorities (and other statutory agencies) in matters of education; community wellbeing; social care and safeguarding of vulnerable individuals (including children and vulnerable adults);
 - collating and exchanging relevant information to achieve joint information sharing objectives in line with legal obligations/requirements and public expectations;
 - co-ordinating resources in respect of the same issue; and
 - supporting Partners in addressing common and locally set priorities and objectives.
 - The Framework provides good practice for the sharing of information between Partners in line with relevant legislation and is an enhancement to other established working practices. It is not intended to restrict the exchange of information between staff working within a Partner organisation. They can/will continue to interact face-to-face, by telephone and/or electronically to carry out their operational duties and responsibilities.
 - This Framework complies with the Data Protection Legislation.

6. Responsibilities

- 6.1 Each Partner, as a Data Controller, must take responsibility for its own decisions to share or not to share data. In addition, each Partner must decide the type and extent of what data and with whom it is appropriate to share in any given situation.
- 6.2 Each Partner, as a Data Controller, is responsible for ensuring that all data they share has been collected and processed lawfully in accordance with the Data Protection Legislation. All Partners will ensure that:
- data is processed lawfully, fairly and in a transparent manner;
 - the requirements for lawful collection and processing of data are met before sharing. If there is a doubt as to the lawfulness of the processing the data should not be shared;
 - where consent is required for data sharing, valid and lawful consent has been obtained from Data Subjects, and Data Subjects have been informed of their right to withdraw their consent;
 - where there is reliance on legitimate interest, that an appropriate Legitimate Interest Assessment has been completed and documented;
 - data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; Further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - all reasonable steps have been taken to ensure that data shared is accurate and up to date before sharing it. If inaccuracy would potentially harm a Data Subject, extra care must be taken to ensure the data is correct and up to date. The Receiving Partner will rely on the currency of that data and if there has been any delay between initial collection by the Providing Partner and use of data by the Receiving Partner, the accuracy of the data must be checked;
 - where information is discovered to be out of date and consequently inaccurate or inadequate, the Receiving Partner agrees to notify the Providing Partner, who will be responsible for correcting the data and notifying all other recipients who must ensure that the correction is made or data are erased or suppressed without delay where appropriate;
 - they accept and understand they may be asked to confirm changes to previously shared data;
 - all Personal Data is kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed;
 - Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of Data Subjects;
 - data is processed in a manner that ensures the security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
 - they ensure the data is of sufficient quality for the intended purpose before the data is shared;

- they agree to cooperate to ensure that all data meets agreed quality standards where specified in an applicable ISA; and
- they take into account any codes of practice, information security policies or best practice guidance within their specific sector that govern the processing of Personal Data.

7. Lead Signatory

7.1 The Lead Signatory is the representative of the Partner from where the Framework originates.

7.2 The Lead Signatory is responsible for:

- the creation of the Framework and retention of the master copy;
- approving suggested amendments to the Framework (paragraph 30.3 – Review and amendments);
- amending the Framework as appropriate and only where amendments are requested and agreed by the Lead Signatory (paragraph 30.3);
- the co-ordination of a full review of the Framework every 5 years;
- establishing an extraordinary review and joint discussion or decision where required (paragraph 30.3.3);
- the circulation of the Framework to parties expressing an interest in becoming a Partner;
- unilateral approval and appointment of new Partners;
- the recording of, and notification to all Partners, of new Partners to the Framework;
- the recording of, and notification to all Partners, of Partners who have withdrawn from the Framework;
- the mediation and resolution of breaches of the Framework where requested by any Partner and the Lead Signatory's decision in such matters is final (paragraph 29 - Dispute Resolution); and
- the termination of the Framework if unanimously agreed by the Partners (paragraph 31 – Framework Termination).

8. Partners

8.1 The signing of this Framework by each Signatory reflects the commitment of each Partner to adopting and complying with the Framework principles and requirements. The Signatory, by signing this Framework, will be agreeing to, for and on behalf of the Partner he/she represents, the terms and conditions of the Framework.

8.2 Each party remains responsible for the data it holds and processes. Once data is shared and safely received from another party, the receiving party will become a Data Controller of that data in its own right. For the avoidance of doubt, the party which shares Personal Data shall also remain a Data Controller for that data.

8.3 Any organisation that requests the regular and routine (systematic) sharing of information will be required to become a Partner, unless such sharing is already governed by an existing information sharing arrangement. If another arrangement is already in place it must be compliant with Data Protection Legislation and consistent with the principles in this Framework.

8.4 It will be the responsibility of the Signatory to ensure that:

- ethical and professional standards are maintained;
- a mechanism exists by which the flow of data can be controlled, and confidentially maintained in addition to ensuring that sharing decisions are recorded and documented;
- staff have appropriate skills and training in data protection;

- adequate arrangements exist within their organisation to ensure the implementation of and adherence to the Framework;
- the legitimate and justifiable sharing of data is lawful notwithstanding any Subject Rights Requests.

9. Nominated Individuals

- 9.1 Each Partner will nominate a suitable individual (being an individual with a good working knowledge of the Data Protection Legislation) to facilitate the operational elements of data sharing between Partners, (he/she shall be termed “the Nominated Individual”). The Nominated Individual can be the same person as the Signatory. Nominated Individuals will:
- 9.2 have a good understanding of the Data Protection Legislation, any other relevant laws and be able to champion data sharing within their own organisation;
- 9.3 act as the first point of contact for any technical problems with sharing the information and, where necessary, report findings to Partners;
- 9.4 initiate internal investigations where the Framework has not been adhered to or there has been a Data Breach;
- 9.5 approve and maintain a record of any individual ISAs entered into under this Framework; and
- 9.6 liaise with the Signatory, where this is a different individual, to review the implementation of and adherence to the Framework.
- 9.7 A full list of Signatories (including the Lead Signatory) and Nominated Individuals is attached at Appendix E.

10. Information Sharing Agreements (ISAs)

- 10.1 All ISAs issued under this Framework will be governed by the principles set out in this Framework, but each will declare its specifics.
- 10.3 Any Partner may issue an ISA under this Framework with existing Partners. Organisations can only sign up to an ISA issued under this Framework if they have joined the Framework in accordance with paragraph 30.1.

11. Other Data Sharing Agreements

- 11.1 The Partners will be provided with a proforma ISA which can be used when sharing data with parties who are not Partners to the Framework, but any such agreement will not be governed by the terms and conditions of this Framework.
- 11.2 Any new data sharing agreement (including those using the proforma ISA) should be lodged with that Partner’s data protection lead/Data Protection Officer (DPO) so that they can track and review all agreements to which the organisation is a signatory.
- 11.3 Partners may enter into data sharing agreements initiated and/or provided by an external organisation, using that organisation’s agreement. It is recommended that the agreement be reviewed to ensure it is consistent and compatible with this Framework and the Data Protection Legislation.
- 11.4 It is a Partner’s sole responsibility to ensure any data sharing agreement they enter in to is appropriate and lawful. If help is needed to produce or review a data sharing agreement, organisations should contact and liaise with their data protection lead/DPO.

12. Data Protection Impact Assessment (DPIA)

- 12.1 A DPIA must be completed alongside any ISA initiated by a Partner, where required to do so (e.g. there is high risk to Data Subjects).

- 12.2 Partners should also consider completing specific DPIAs to aid their decision making if they are being asked to share high risk data.
- 12.3 If a sharing risk is identified by a Partner about their own organisation, they will be required to alert the Lead Signatory and should mitigate any risk. They may need their DPO/data protection lead to sign off that this has been done and must alert the Lead Signatory to confirm this.
- 12.4 If a data sharing risk is identified in a Partner organisation and risk mitigation is not undertaken, the Lead Signatory may suspend data sharing arrangements with that Partner.

13. Sharing and disclosing data

- 13.1 Personal Data must only be shared where it is reasonable, necessary, proportionate, relevant, justified and on a 'need to know' basis.
- 13.2 Partners will always consider alternatives to sharing Personal Data in the first instance, e.g. Anonymisation or Pseudonymisation.
- 13.3 This Framework does not grant unrestricted access to information another Partner may hold. It provides the parameters for the safe and secure sharing of Personal Data on a justifiable 'need to know' basis. Signing the Framework does not mean that a Partner is obliged to share all or any data with another Partner.
- 13.4 Where a 'dataset' is being shared (i.e. structured data), it will be accompanied by a table providing definitions of the data fields if these are not self-explanatory, to ensure that the meaning of the data provided is clearly understood by all users
- 13.5 An information sharing flow chart is provided separately to assist Partners in decision making in respect of data sharing.

14. Shared or integrated systems

- 14.1 Partners may use a number of internal shared systems, for example between dioceses and bishops' offices, or national systems which are owned and maintained by the NCIs. In both case the diocese or the NCIs act as agents on behalf of the Partners in having signed contracts and relevant data processing agreements with contractors and suppliers, and in providing system development, maintenance and support services.
- 14.2 Agency means the following:

- 14.2.1 The NCIs or relevant other Data Controller shall be entitled to act as agent of the Partners for the following purposes:
 - a. operational and technical discussions relating to the Services and Software including but not limited to maintenance and data protection matters;
 - b. delivery of instructions relating to the Services and Software;
 - c. negotiating and giving agreement to be bound by a data processing agreement (and any replacement or variation of such an agreement) and any support and maintenance Agreement in the name of, and on behalf of, the Partner.
 - d. acting as system administrator for the purposes of providing first line support for operational users and managing necessary maintenance/upgrades to the system.
 - e. undertaking reviews of breach management by suppliers as necessary to ensure data is secured and protected as required by the UK GDPR or the EU GDPR as the case may be.
 - f. undertaking audits or requesting additional information from suppliers as necessary to ensure their continued compliance with Article 28 of the UK GDPR or EU GDPR as the case may be.

- g. investigating data breaches such that it can conclude whether the supplier has sufficiently identified and mitigated the breach depending on the specific circumstances. Only the following details will be provided where the breach does not specifically affect the NCIs data:
 - 1) the cause of the breach (technical, cyber security, human action)
 - 2) the source of the breach (supplier or the data controller)
 - 3) the severity and impact of the breach (risk to data subjects)
 - 4) the mitigation of the breach (organisational or technical measures to limit or minimise impact, and prevent recurrence)
- 14.3 Shared systems allow various user types (including Partners etc) to access and use the system to process their own data, which should be segregated by user type. The Data Controller which owns a relevant shared system has access to this data for the purposes of support and maintenance, or for the purposes specified in a relevant ISA. It is the responsibility of Partners to ensure appropriate access controls are in place.
- 14.4 Sharing of segregated data in a shared system can be provided either by a Data Controller extending access to that data on a case by case basis to other Partners. The default position is that segregated data must only be shared with the agreement of the relevant Data Controller either through an ISA, or by using the Ad-hoc Data Sharing Request Form (Appendix C), except where such data is being processed by the relevant Data Controller for the purposes of recruitment, payroll, HR services, the National Clergy Register or Crockford's, and/or as stated in a relevant ISA.
- 14.5 Sharing of data with internal or external IT services must be managed by the Partner responsible for the shared system under appropriate contracts, data processing and/or access agreements.
- 14.6 Where data is transferred automatically between systems, via an integration platform, such data is shared data and is covered by the terms of this Framework, and any relevant ISAs.
- 14.7 Where a Partner accesses, operates or administers shared or integrated systems on behalf of another Partner, this Framework, and any appropriate ISA, shall apply to that incidental access to Personal Data.
- 14.8 Each Partner which uses a shared system remains responsible for their Personal Data in any such system and shall remain as the Data Controller in respect of that Personal Data.

15. Ad-hoc Information Sharing

- 15.1 The Framework and ISAs are designed to cover the sharing of data where there is a regular need for the exchange of Personal Data between Partner organisations. There will be circumstances in which the sharing of Personal Data may be required to facilitate a specific one-off task between Partner organisations which is not covered by an ISA. This must be done with the use of an Ad-hoc Data Sharing Request Form. This is designed to record the specific instance of sharing data. The proforma form is provided at Appendix C. See paragraph 18 below.
- 15.2 The Partner receiving the request must indicate their agreement to share on the form, and return the signed and dated form to the requesting Partner with the shared data where appropriate.
- 15.3 Partners should keep copies or records of any Ad-hoc Data Sharing Request Forms received or provided to other Partners.

16. One-way disclosure of information

16.1 Generally, this Framework and supporting ISAs will facilitate the two-way sharing of information. Sometimes it may be necessary to share a set of data in one direction. In cases where both Partners are signed up to this Framework then an ISA can be drawn up for the specified purpose. However, if the organisation who wishes the information to be disclosed is not a party to the Framework and the sharing is not regular and routine then it may be more appropriate to use an Ad-hoc Data Sharing Request Form.

17. Authorisation

17.1 Each Partner shall ensure all data sharing activity by a Partner is appropriately authorised by the individual who has responsibility for the processing of the relevant Personal Data.

18. Requesting data

18.1 If a Partner requests the sharing of Personal Data from another Partner where an ISA is not in place, they should use the Ad-hoc Data Sharing Request Form. The Partners will not seek to override the procedures which each Partner has in place to ensure that data is not shared/disclosed illegally or inappropriately.

18.2 It is acceptable for a Providing Partner to obtain further details from the Partner requesting the information to satisfy itself that such a Partner can process the information lawfully and securely.

18.3 The extent of the data shared must be restricted to only that Personal Data which is necessary to enable the Receiving Partner to achieve its objectives.

18.4 It is the responsibility of the Providing Partner to inform Data Subjects of any data sharing via a suitable Privacy Notice or other means, unless there is a legal or justifiable reason not to do so.

19. Decision not to share

19.1 Where a Partner to this Framework chooses not to share information, they must provide a full and clear written explanation of the reasons the sharing request has been refused to the requesting Partner. The Lead Signatory should be informed if there is a dispute in relation to a decision not to share (see paragraph 29 below on **Dispute Resolution**).

20. Use of Shared Data

20.1 A Partner in receipt of data must:

- only use data for the purpose it was originally shared; and
- not use that data in such a way that it is likely to be detrimental to a Data Subject (unless the circumstances warrant such use). If the proposed purpose is incompatible with the original purpose under which the data was collected, or if the Data Subject objects to the new processing purpose, then that information must not be used for the proposed purpose until another lawful basis has been established, or the objection resolved.

21. Third Parties:

2.1 Where information is shared at meetings (and particularly where organisations attending the meeting are not parties to the (Framework) it is good practice to remind participants of the confidential nature of the information being shared. Where such information involves Personal Data, proper data protection principles must be applied where relevant to discussions and any notes or minutes taken. It may also be necessary for attendees who are not from Partner organisations to sign a

confidentiality and data protection agreement so that information is not disclosed unlawfully outside the meeting.

22. International transfers

22.1. Personal Data may only be transferred between the UK and EU/EEA countries or where an adequacy arrangement has been entered into for that territory. No transfer is allowed to the territories not covered by an adequacy arrangement (such as the United States of America) unless specific and adequate protections are in place (such as Standard Contractual Clauses). Any Partner uncertain of their position should seek advice and guidance from their DPO/data protection lead.

23. Data handling and management

23.1 Storing and security

23.1.1 All Partners will put in place procedures governing the secure storage of all Personal Data retained within their manual or electronic systems.

23.1.2 Partners should (in respect of the Personal Data for which they are Data Controller) have appropriate policies which should include data protection, records management and information security.

23.1.3 Partners should also provide relevant policies to other Partners upon request.

23.2 Security requirements

Security requirements should include the following restrictions:

- data must be stored securely, with appropriately restricted access, and on encrypted devices or systems;
- data must not be stored on personal mobile devices such as phones or tablets;
- data must not be stored on removal media such as memory sticks, except for transfer purposes; and all data that may be received initially via a mobile device must be transferred as soon as possible to the organisation's IT system;
- anonymise, pseudonymise or aggregate Personal Data where appropriate;
- appropriate security management (e.g. encryption, authentication, policies, procedures, staff training);
- appropriate access controls to electronic and manual systems;
- appropriate physical and environmental security to buildings and other hardware;
- appropriate back up and disaster recovery systems;
- only retain the data for as long as specified in the ISA, if specific retention rules have been included;
- dispose of the data in the most secure way possible, if required in the ISA once the ISA ends/is terminated in accordance with its provisions.

23.3 Retention and Disposal

23.3.1 All Partners will put policies and procedures in place governing the retention and destruction of records containing Personal Data retained within their manual and/or electronic systems.

- Partners will ensure that any out-of-date information that still needs to be retained, but is not permanently deleted, is safely archived, or put "offline".
- The following destruction/disposal processes will be used by all Partners when the information reaches its disposal date:

- **Paper-** confidential shredding and proper disposal of shredded paper. If a Partner is not using an external shredding service, they must ensure that paper is shredded and disposed of in such a way as to prevent reassembly of information i.e. not put into recycling containers, not disposed of in a public place. Shredded paper may be pulped in water prior to disposal if confidential shredding and disposal is not available.
- **Electronic data (emails, MS Office documents, scanned documents etc) –** Ensure that data is deleted from all relevant folders – i.e. delete the document or email, then empty the recycle bin or deleted items folder. For advice on electronic shredding contact your IT department or service.
- **Structured data –** suitable and appropriate rules must be in place to manage database records, such as manual or automated retention rules and the deletion of case records. If records cannot be deleted from systems, other measures must be taken to ensure these records are inaccessible or suppressed (i.e. can no longer be processed).

24. Transfer methods

- 24.1 All Partners will ensure the secure exchange of information. Partners should put in place policies and procedures that govern the secure transfer of Personal Data, this includes transferring information internally within their organisation and to other Partners as well as externally to third parties.
- 24.2 Details of the methods of transfer used and all subsequent security measures must be included on any individual ISA.
- 24.3 Partners are responsible for ensuring that electronic and hard copy information that is shared under any ISA will be transferred securely between participating organisations/individuals, using adequate and suitable technologies or processes i.e. encryption, courier etc.
- 24.4 The following transfer mechanisms are acceptable under the terms of this Framework:

Automated	Automated data transfer from system to system via secure network.
System based transfer	Appropriate shared access to data within a case management system (read only, edit).
Courier	Paper documents sent or received by courier.
	Encrypted removable media e.g. CD / DVD / memory stick.
Email	Email address is confirmed and accurate. Limited use of “cc”; use of “bcc” only where necessary for those to be included.
	Password protected documents.
Encryption	Encrypted email solution (e.g. Egress) or where email is encrypted and used only within the organisation (e.g. 0365 Outlook), or where end to end encryption is in place between organisations.
	Documents are encrypted using 7zip or similar software, where there is no cost to recipients.
	Encrypted portals which have been approved for use (WeTransfer etc) and which are UK or EU based.

Hand delivered/ Recorded or Tracked Post/Courier	By known persons or courier.
	Encrypted removable media.
	Media/ documents in tamper-free sealed envelope/ box/ container and fully addressed.
	Tracked post - Special Delivery/Recorded Signed for).
Manual transfer	Manual transfer by authorised individuals only.
	Upload or download via secure link to secure system or site or portal.
	Documents on secure app/website.
Text	On encrypted mobile phones only or where data is segregated from users' Personal Data.
	Mobile phone numbers are accurate and confirmed.
	Data must be transferred to other secure locations and deleted from senders' phone as soon as possible.

24.5 The following transfer mechanisms are not acceptable for the sharing of Personal Data between Partners under the terms of this Framework:

- fax;
- untracked/untraceable mail;
- any other method not listed in the above table.

25. Subject Right Requests and complaints

25.1 Data subjects have rights in respect of their Personal Data, and where relevant all parties to an ISA must comply. Where a Partner is the recipient of a Subject Rights Request it is that Partner's responsibility to lawfully comply with that request in accordance with the Data Protection Legislation, the terms of this Framework and any applicable ISA.

25.2 Each Partner will ensure that they have effective procedures for dealing with Subject Rights Requests and complaints from individuals in relation to the use and disclosure of Personal Data. All Partners who are party to the Framework must provide cooperation and assistance to each other in order to resolve any Subject Rights Request or complaint involving shared data.

26. Appropriate Policy Document

26.1 All Partners must have in place an appropriate policy document outlining their compliance measures and retention policy if processing Special Category Data and/or Criminal Offence Data as required by the Data Protection Act 2018 Schedule 1, Part 4.

27. Training and awareness

27.1 All Partners will ensure that the individuals within their organisations who have access to shared data have adequate knowledge, training and skills to enable them to share information legally; comply with any professional codes of practice and local policies and/or procedures, including this Framework. Training should take place at the earliest opportunity before any access to Personal Data is granted and a refresher should be undertaken at regular intervals, e.g. annually or bi-annually. Individuals must understand what they are expected to do when:

- sharing with other members of their team;
- sharing with other parts of their organisation;
- there is a need to ask a Data Subject for permission to share their data;
- there is a need to transfer Personal Data securely;
- a Data Subject objects to the ways his/her Personal Data is being used or shared, (what action do they need to take);
- they can share information without a Data Subject's consent or override any objection.

27.2 All Partners will take reasonable steps to ensure that all those that are involved in the information sharing process are aware of, and comply with, their responsibilities and obligations with regard to:

- the confidentiality of Personal Data;
- the commitment of the relevant Partner organisation to only share information legally and within the terms of an agreed individual ISA;
- only sharing information where necessary, justified, proportionate, relevant, on a need to know basis and securely;
- the consequences of the disclosure of Personal Data which cannot be justified, whether inadvertently or intentionally;
- the process for reporting any unauthorised disclosure (see paragraph 28 below - Breach Management).

28. Breach Management

28.1 All Partners will have appropriate measures in place to investigate and deal with Data Breaches. If it is established that a Data Breach has occurred involving shared data, the Partner making the discovery shall inform the Partner(s) who are subject to or affected by the Data Breach of the details within a reasonable timescale, 24 hours where possible, using the Breach Reporting Form proforma as provided at Appendix D.

28.2 Following this, any Partner(s) who has suffered a Data Breach shall:

- investigate the cause of the Data Breach and establish the impact;
- where appropriate, take any necessary action in accordance with its legal responsibilities; and
- take appropriate steps to mitigate the cause and avoid any repetition.

28.3 The Providing Partner will also assess any potential implications for the Data Subject whose information has been compromised and if necessary:

- notify the Data Subject concerned;
- inform the Data Subject of their statutory rights; and
- provide the Data Subject with the appropriate support.

28.4 Where a Data Breach has occurred the Partner which is the subject of the Data Breach, supported by other Partners as necessary, must also notify the ICO within 72 hours unless the Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subject(s). It is the responsibility of the Partner managing an incident to investigate and report as appropriate to any other necessary regulatory bodies, e.g. Police, Charity Commission etc.

29. Dispute Resolution

- 29.1 If any Partner to this Framework believes that any other Partner is acting in breach of the Framework, the Nominated Individuals of the Partners involved will discuss the issue with each other and attempt to resolve it.
- 29.2 Any Partner may ask the Lead Signatory to help resolve the issue. In such circumstances, the decision of the Lead Signatory is final, and may include removal of that Partner from the Framework and any relevant ISAs.
- 29.3 If no resolution can be reached, the Partner in breach will be expected to notify the Lead Signatory and withdraw from the Framework and any relevant ISAs. Any other Partner may also withdraw from this Framework in response to the breach and cease to provide or receive data under any relevant ISAs. The Lead Signatory will inform all Partners that a Partner has withdrawn from the Framework, however, it is the responsibility of the individual Partners to withdraw themselves from relevant ISAs.

30. Processes

30.1 Joining as a Partner

- 30.1.1 Any organisation wishing to become a Partner to this Framework may obtain a copy of the Framework from the Lead Signatory. Applications to become a Partner should be made to the Lead Signatory. The Lead Signatory will decide whether to add the applicant as a Partner, make any necessary amendments to the documentation, obtain a signature and inform other Partners/organisations. Becoming a Partner to this Framework does not infer any right or obligate any Partner to automatically exchange information with another Partner without the relevant ISA's being agreed and in place.

30.2 Leaving the Framework

- 30.2.1 Any Partner may leave the Framework at any time by providing 1 (one) month's written notice to the Lead Signatory. Where a Partner leaves the Framework, they will be considered to have also left any applicable ISAs, and no further information will be shared with them.
- 30.2.2 As a Receiving Partner will become the data controller for the Personal Data it has received under this Framework, it is that Partner's responsibility to manage that data, (e.g. decide how long to retain that data). However, in some cases, the Providing Partner may require the Receiving Partner to return and/or securely destroy Personal Data. If that is the case, this must be specifically stated in the ISA, including any specific limitations and controls on the Personal Data that is shared, (e.g. when/how the Personal Data must be destroyed). An undertaking must be given by the Receiving Partner that any limitations and controls have been met within 1 month of notification of termination. Exceptions to this must be agreed with the Lead Signatory and the Receiving Partner(s).

30.3 Review and Amendments

- 30.3.1 Responsibility for the review and updating of this Framework and any ISA lies with the Lead Signatory.
- 30.3.2 If Data Protection Legislation changes in a way that the Lead Signatory deems the Framework no longer adequate for the purpose of governing lawful data sharing, the Lead Signatory shall amend or vary the Framework as they deem appropriate.
- 30.3.3. A Partner can request an extraordinary review by the Lead Signatory in consultation with the other Partners at any time where the Partner believes, acting reasonably, that a joint discussion or decision is necessary to address any particular issues or developments significantly affecting the effectiveness of the Framework i.e. prevents appropriate sharing, breaches Data Protection Legislation, or poses a high risk to Data Subjects.

30.3.4 Any review undertaken will ensure that:

- the contact list of Partners is current and up to date (as far as reasonably practicable);
- the Framework is still useful and fit for purpose; and
- any emerging issues have been identified and consider whether the information sharing is still necessary, proportionate, justified, relevant, accurate and secure.

30.3.5 A Review and re-issue of the Framework or the ISAs due to a change in process or law will not require Partners to sign up again.

31. Framework Termination

31.1 The Framework and any ISA will remain in force until terminated. A Partner cannot unilaterally terminate the Framework but may withdraw from it (see paragraph 30.2).

31.2 The Framework can only be terminated by the agreement of two-thirds of the Partners. Notice will be served by the Lead Signatory to all Partners, and the Framework will end after 1 month of notice being served.

31.3 Termination of the Framework automatically terminates all related ISAs and all sharing of data under the relevant ISAs must cease.

32. Indemnity

32.1 Each Partner indemnifies each other and shall hold each other harmless from any costs, charges, damages, expenses or loss which they cause each other as a result of any breach of any of the provisions of this Framework or any applicable ISA.

Appendix A - Definitions (alphabetic)

The following definitions and rules of interpretation apply in this Framework.

Terms shown below in bold and throughout the Framework are defined terms for the purposes of interpretation and shall have the meaning set out below or as otherwise defined throughout the Framework.

Singular terms include plural and vice versa.

Headings and Titles are not defined terms unless otherwise set out below and do not form part of the operation of the Framework and are for reference only.

Ad-hoc Information Sharing

Sharing information not covered by Sharing Agreements on a one-off basis, or disclosure without the Data Subject's knowledge.

Anonymisation

The process by which all identifiable information is removed from a set of data, (i.e. anonymised). Such data will no longer be Personal Data.

Church

Refers to the institutional Church of England and the Representative Body of the Church in Wales.

Church Officer

A Church Officer is anyone appointed/elected by or on behalf of the Church to a post or role, whether they are ordained or lay, paid or unpaid.

Criminal Offence Data

Personal data relating to criminal convictions and offences or related security measures, including criminal activity; allegations; investigations; and proceedings.

Data Breach

The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, Special Category Data and/or Criminal Conviction Data.

Data Controller

A body or organisation that makes decisions on how Personal Data is being processed.

Data Processor

A body or organisation that processes data on behalf of, and only on the instructions of, a Data Controller. Processors do not make decisions about the purposes and means of the data processing, but may determine how the data should be processed. Processing by a Data Processor must be governed by a contract or Data Processing Agreement.

Data Processing Agreement

The contract between a Data Controller and a Data Processor, specifying work to be carried out on behalf of a Data Controller.

Data Protection Legislation

All applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Information Commissioner or other relevant data protection supervisory body/regulator.

Data Subject

The individual to whom the data being processed relates and is identified/identifiable by that data.

Further Processing

The processing of Personal Data for purposes other than those for which the Personal Data were initially collected. This can be allowed only where the processing is compatible with the purposes for which the Personal Data were initially collected.

Information Sharing Agreement (ISA)

An Information Sharing Agreement/ISA is a document that sets out in detail any information sharing arrangements between parties who have signed up to the Framework.

Information Sharing Framework

An Information Sharing Framework is a high-level document between Data Controllers to agree the terms and conditions under which they will share Personal Data.

Information Sharing Register

A Register that lists the details of all information sharing arrangements agreed or entered into by that Data Controller. The Register may be requested by the ICO in the event of a complaint.

Lead Organisation

The organisation which owns the Framework and any related documents stemming from it, and which initiates the circulation of the Framework and ISA to other Data Controllers who wish to enter into information sharing arrangements with it.

Lead Signatory

The individual signing the Framework on behalf of the Lead Organisation, i.e. the organisation from whom the Framework originated. This may or may not be the same individual who is signing the ISA (see Nominated Individual below).

Nominated Individual

The individual in a Partner organisation who is responsible for practical implementation of the Framework and the ISA. This may be the same individual as the Signatory (or Lead Signatory in the case of the Lead Organisation), although this is not essential. Nevertheless, he/she should be directly involved in the data processing activities described in the ISA.

Partner(s)

An organisation (i.e. Data Controller) which is party to the Framework and ISAs.

Personal Data

Any information that relates to a Data Subject, including any information which can be used to identify a Data Subject.

Privacy Notice

As stated in Articles 13 and 14 of the UKGDPR: information to be provided to data subjects where Personal Data is collected from the Data Subject or a 3rd party.

Providing Partner

The Partner who is the organisational source of Personal Data and shares it with one or more other Partners. This is the Data Controller responsible for the initial collection of that data.

Pseudonymisation

The process of removing any identifiable information from a data set but in such a way that it can be re-identified if required. Usually done with a reference number, (i.e. pseudonymised).

Such data will still be Personal Data, although it offers an extra layer of protection and will help satisfy security requirements.

Receiving Partner

The Partner who receives Personal Data from one or more other Partners.

Signatory

An individual signing the Framework on behalf of a Partner.

Special Category Data

Specific types of Personal Data that require additional care being taken when processing. The categories are:

- data revealing racial or ethnic origin;
- data revealing political opinions;
- data revealing religious or philosophical beliefs;
- data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Subject Rights Request

The exercise by a Data Subject of their rights under the Data Protection Legislation, including the right to:

- be informed about the collection and the use of their Personal Data;
- access Personal Data and supplementary information;
- have inaccurate Personal Data rectified, or completed if it is incomplete;
- request erasure (to be forgotten) in certain circumstances;
- restrict processing in certain circumstances;
- data portability, which allows the Data Subject to obtain and reuse their Personal Data; for their own purposes across different services;
- object to processing in certain circumstances;
- object to automated decision making and profiling;
- withdraw consent at any time; and/or
- complain to the Information Commissioner or seek judicial remedy.

Appendix B - Ad-hoc Data Sharing Request Form

For use by the organisation (Data Controller) making an ad-hoc or one-off request for data that is not covered by an Information Sharing Agreement (ISA). This form should not be used for regular and systematic information sharing.

Please complete and send this form to *[insert email address]*.

Data Sharing Request Form

Name of organisation/ department to whom request is addressed	
Name of organisation making request	
Name and position of person requesting data	
Date of request	
Is there an information sharing agreement in place?	Yes / No
Does the processing involve special category or criminal offence data (or law enforcement processing)?	Yes / No

Description of data requested

Purpose of sharing

Lawful basis/bases for disclosure. Please include any conditions for processing special category or criminal offence data. If Legitimate Interest is a lawful basis, please include a copy of the Legitimate Interest Assessment.

Are there any circumstances in the requested sharing that might result in the risk to individuals? How will these risks be mitigated?

How the information will be disclosed

Please enter the details for how the information should be disclosed i.e. use of secure post, encrypted email etc.

Data sharing decision by data controller

Has the DPO/ Data Protection Lead been consulted?	Yes / No
---	----------

Has a DPIA been considered?

DPIA undertaken and outcome (if applicable)

Was the information shared with or without the consent of data subjects?

What arrangements are there for complying with an individual's information rights?

What do you need to tell people about sharing their data and how you will communicate that (Privacy Notice).

Are there any specific arrangements needed to comply with information rights request?

What retention/deletion arrangements have been agreed?

Disclosure agreed	Yes / No
Reason/s for sharing or not sharing	
Disclosure authorised by	
Data disclosed by	
Date of disclosure	

A copy of the completed and signed form should be retained by both data controllers.

Appendix C - Breach Reporting Form

If it is established that a Data Breach has occurred, the Partner making the discovery shall inform the Partner(s) who are subject to or affected by the Data Breach of the details within a reasonable timescale, 24 hours where possible, using this Form. See paragraph 28 of the Framework for further details.

Name of individual reporting the breach		Date	
Organisation/Department		Manager	
Time since breach	0-72 hours		Over 72 hours
When the breach occurred	Date:		Time:
When you became aware of the breach	Date:		Time:
Was the breach caused by a cyber incident?	Yes / No (If Yes, please provide details)		
Type of Breach	Select one or more: Disclosed in error (accidental); lost data or hardware; lost in transit; non-secure disposal; technical failure/fault; procedure/process failure; unauthorised access or use; misuse of data; other (please describe).		
Description of the breach	Free text - please enter all relevant details (including how did it occur, what was the source of the breach, who is responsible for the breach).		
What type of data has been breached?	Provide details e.g. Name, E-mail, address, phone number, financial information, racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic data, data concerning health, data concerning sex life, criminal conviction/offence data. How many records were included?		
Was the data protected?	Yes / No Provide details (encrypted, password protected etc)		
If accidental disclosure, has the unintended recipient confirmed deletion/return of the data?	Yes / No Provide any further details.		
Who has been affected?	Provide details e.g. Staff, former staff, consultant, unconnected third party, child/minor, vulnerable adult; how many data subjects are affected.		
What are the possible consequences?	Consider: loss of control of personal data, limitation of rights, discrimination, identity theft or fraud, financial loss and other economic or social		

	<i>disadvantage. How severe or significant are the consequences?</i>
What action has been taken to mitigate the effects?	<i>Consider: actions to reduce effect on data subject, actions to control breach and avoid impact on other data subjects.</i>
Has the data subject been notified?	<i>Provide details. If no notification, please explain why not.</i>
Data protection training	<i>Provide details of training undertaken by the person responsible for the breach.</i>
What you have learned?	<i>Provide details of changes you will make to processes or behaviour to ensure this does not happen again</i>
Has this type of breach occurred before?	<i>Provide details, including whether previous breaches were the result of the actions of the same individual.</i>

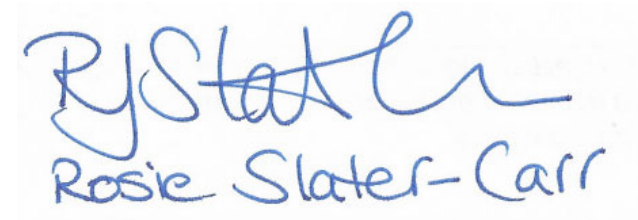
To be completed by the Data Protection Team

Recorded on breach register?	Yes/No
Is this a reportable breach?	Yes/No <i>(if No, explain why)</i>
Reported to ICO / Date	Yes/No <i>(initial and/or final report?); ICO Reference number</i>
Reported to Charity Commission / Date	Yes/No <i>(initial and/or final report?); CC Reference number</i>

A copy of the completed form should be retained by affected data controllers, and the details entered in a breach register, or used to inform a notification to the ICO.

Appendix D - Signatories and Nominated Individuals

Lead Signatory – Rosie Slater-Carr, Chief Operating Officer, Church of England Central Services



Rosie Slater-Carr