



Church of England National Safeguarding Information Sharing Agreement

VERSION 1.0

JANUARY 2022

Contents

Summary Sheet.....	4
1.0 Introduction	5
2.0 Aims and Objectives	5
3.0 Partners and Scope	7
4.0 Lawful Bases for Sharing	7
5.0 Data categories	9
6.0 Specific Requirements and Restrictions.....	9
7.0 Core group or safeguarding risk management meeting.....	9
8.0 Anonymised and Pseudonymised Information	10
9.0 Data Protection Impact Assessment (DPIA).....	11
10.0 Signatures	11
Appendix A Lawful bases	12
Appendix B Policies.....	19
Appendix C Data Protection Impact Assessment.....	20
Appendix D Privacy Notice.....	22
Appendix E Signatures	29

Approval and review

Approved by	Director of Safeguarding, National Safeguarding Team (NST)
Document owner	NCIs Information Governance Officer
Document author	NCIs Information Governance Officer; NCIs Legal Office' Stephens Scown LLP
Date	9 February 2022

Version Control

Version No	Revision Date	Amended by	Summary of Changes
0.1	March 2019	NCIs Information Governance Officer	Draft agreement for consultation with dioceses and cathedrals
0.2	May 2019	NCIs Information Governance Officer	Amended lawful bases, removed Anonymisation Guidance, minor clarifications following consultation.
0.3	May 2020	NCIs Information Governance Officer	Revised to bring in line with ICO guidance
0.4	June 2021	NCIs Information Governance Officer	Amended lawful bases, added amendments from 2019 consultation

0.5	August 2021	Stephens Scown LLP	External review, revision and consolidation
0.6	September 2021	NCIs Information Governance Officer; NCIs Legal Office; Lupton Fawcett LLP	Internal legal review of Stephens Scown amendments; final amendments for consultation version, addition of appendices; revision of Isle of Man Data Protection Legislation
0.6	January 2022	NCIs Legal Office	Addition of safeguarding supervision purpose and lawful bases
v1.0 Final	January 2022	NCIs Information Governance Officer; NCIs Legal Office	Amendments following consultation, revisions relating to the new Code of Practice. Approved

Summary Sheet

Title of Agreement	Church of England National Safeguarding Information Sharing Agreement
---------------------------	--

Purpose	To facilitate the sharing of safeguarding information between the organisations listed below. The purpose of the information sharing is to protect children and vulnerable adults from abuse within the Church of England.
----------------	---

Lead Organisation	Archbishops' Council
--------------------------	----------------------

Lead Signatory	Director of Safeguarding, National Safeguarding Team (NST)
-----------------------	--

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 and 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 which are signatories to this agreement.</p>
-----------------	---

Date agreement comes into force	1 March 2022
--	--------------

Date of agreement review	February 2025
---------------------------------	---------------

Agreement drawn up by:	NCIs Data Protection Officer; NST; NCIs Legal Office; Church in Wales Legal Office; Stephens Scown LLP; Lupton Fawcett LLP.
-------------------------------	---

Stakeholders consulted:	Select group of dioceses and cathedrals
--------------------------------	---

1.0 Introduction

- 1.1 This Information Sharing Agreement (**ISA**) has been drawn up under the umbrella of the Church of England's Data Sharing Framework (**Framework**) which sets out the core information sharing principles that have been agreed by the Partners.
- 1.2 The principles, rules, mechanisms and terms and conditions of the Framework apply to any data sharing that takes place under this ISA.
- 1.3 The ISA is designed to facilitate the sharing of safeguarding information between the Partners. It is incumbent on all Partners to recognise that any information shared must be justified and in accordance with the terms and conditions of this ISA. The balance between a Data Subject's rights and freedoms and the need to disclose Personal Data must be assessed to ensure the data shared between Partners is proportionate to the purpose. Anyone in doubt should consult their Nominated Individual before proceeding.
- 1.4 Definitions used in this ISA are as defined within it except where already specified in the Framework.
- 1.5 Data sharing is essential for effective safeguarding and promoting the welfare of children, young people and vulnerable adults. It is a key factor identified in many serious cases where inadequate data sharing has resulted in missed opportunities to take action that keeps children, young people and vulnerable adults safe and/or Data Breaches.
- 1.6 Data sharing for effective safeguarding is a requirement of safeguarding guidance issued by the House of Bishops under section 5 of the Safeguarding and Clergy Discipline Measure 2016 (the 2016 Measure). In such circumstances, the persons and bodies listed in section 5 (e.g. bishops, diocesan boards of education, cathedral chapters etc.) must pay "due regard" to such guidance, which will include any obligations to share. "Due regard" means that they are not free to disregard House of Bishops' guidance but are required to follow it (e.g. share information in given circumstances set out in the guidance) unless there are cogent reasons for not doing so. 'Cogent' for this purpose means clear, logical and convincing. The Safeguarding (Code of Practice) Measure 2021 (the 2021 Measure) replaces and strengthens the duty to have due regard to House of Bishops' safeguarding guidance with a duty to comply with the requirements in a new safeguarding code of practice (the Code). Relevant policies and guidance are provided in Appendix B.
- 1.7 The overall objectives for sharing Personal Data in respect of safeguarding is to protect children and vulnerable adults from abuse within the Church of England (including, but not limited to, the Partners) and to ensure their safety, welfare and wellbeing.
- 1.8 A template Privacy Notice (PN) governing the sharing of safeguarding data is provided in Appendix D. All Partners must adapt the Privacy Notice to include their contact details, logo's etc, and ensure that PN is easily available to Data Subjects online, or is provided to them.

2.0 Aims and Objectives

- 2.1 The aim of this ISA is to ensure that all Partners who are responsible for safeguarding are able to fulfil their responsibilities to victims, survivors, respondents, families of those affected, and the general public.

- 2.2 The purpose of this ISA is to enable Personal Data, Special Category Data and Criminal Offence Data to be shared between Partners where both Partners are Data Controllers (each Partner exercises overall control over the purposes and means of processing Personal Data).
- 2.3 The further purpose of this ISA is to enable information to be shared between the Partners in support of the following objectives and benefits, including but not limited to:
 - 2.3.1 promoting and maintaining a safer culture within the Church that protects and promotes the welfare of children, young people and vulnerable adults as required by “Promoting a Safer Church”;
 - 2.3.2 creating and maintaining environments that are safer for all, that promote well-being, that prevent abuse, and that create nurturing, caring conditions within the Church for children, young people and vulnerable adults and help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour;
 - 2.3.3 preventing death or serious harm;
 - 2.3.4 to enable the Church of England Pensions Board housing service to put in place safeguarding risk management or support arrangements (with other agencies and Diocesan safeguarding teams as necessary);
 - 2.3.5 to enable the Church of England Pensions Board housing service to support other agencies in carrying out their statutory functions (e.g. prevention of crime), including the need to process criminal offence data to ensure we house you appropriately if you are currently under supervision of a statutory authority
 - 2.3.6 the safer recruitment of all those with any responsibility in a Partner relating to children, young people and/or vulnerable adults within the Church;
 - 2.3.7 training and equipping Church Officers to have the confidence and skills they need to care for and support children, young people and vulnerable adults, including recognising and responding to abuse and identifying low-level concerns that may reveal people at risk of abuse;
 - 2.3.8 responding to every safeguarding concern or allegation appropriately and recording all safeguarding work; coordinating effective and efficient responses and preventing abuse and harm that may increase the need for care and support.
 - 2.3.9 reporting all suspicions, concerns, knowledge or allegations, that reach the relevant threshold, to the appropriate statutory authorities irrespective of the status of the person;
 - 2.3.10 offering care and support to all those who are known to have been abused or allege abuse, or are considered to be vulnerable to abuse regardless of the type of abuse, when or where it occurred and to help people access support to reduce risk and promote wellbeing, including making a suitable apology when required or considered necessary;
 - 2.3.11 offering care and support to all those who are the subject of safeguarding allegations or investigations and help people to access support to reduce risk and promote wellbeing;
 - 2.3.12 taking responsibility for ensuring that steps are taken to protect others when any Church Officer and any individual regularly involved with a Church body is

- considered a risk to children, young people and vulnerable adults and enabling early interventions to prevent the escalation of risk;
- 2.3.13 working to mitigate any identified risks in collaboration with the relevant statutory agencies in accordance with relevant law;
 - 2.3.14 provision of professional supervision by the National Safeguarding Team to persons with operational responsibility for safeguarding in Partners;
 - 2.3.15 providing reports to local, national or statutory bodies responsible for oversight of safeguarding within Partners;
 - 2.3.16 liaison with internal and external advisers for the purpose of litigation, dispute resolution, judicial process or or to process information related to an insurance claim;
 - 2.3.17 providing anonymised copies of Serious Incident Reports to the National Safeguarding Team;
 - 2.3.18 undertaking investigations and reviews (including lessons learnt reviews) and engaging in peer support to maintain and improve good practice in safeguarding; understanding failings in particular cases or safeguarding practice; improving processes and case management and revealing patterns of abuse that were previously undetected and that could identify others at risk of abuse;
 - 2.3.19 maintaining accurate and up to date information on: Disclosure and Barring Service (DBS) checks; training and post/positions held by anyone within a Partner with any responsibility relating to children, young people and vulnerable adults;
 - 2.3.20 research purposes in order to quality assure safeguarding practice and inform strategic planning on safeguarding, for example, the conduct of lessons learnt reviews.

3.0 Partners and Scope

- 3.1 This ISA is between the Partners.
- 3.2 If a **new Partner joins the ISA**, their details and signature will be added to the master version of the ISA by the Lead Signatory and all Signatories will be informed as soon as reasonably possible.
- 3.3 If any **Partner objects to the inclusion** of the new Partner, they should contact the Lead Signatory within one month following notification, stating their reasons. The Lead Signatory will make the final decision with regard to any new inclusion.
- 3.4 If a **Partner leaves the ISA**, their details will be amended to indicate this on the master version of the ISA held by the Lead Signatory and all Signatories will be informed within one month, or as soon as reasonably possible.

4.0 Lawful Bases for Sharing

- 4.1 Personal Data is shared under the terms of this ISA on the valid lawful bases as set out in Appendix A. For the avoidance of doubt, it may be the case that not all valid lawful bases as set out in Appendix A will apply to every instance of data sharing. Other valid lawful basis/bases may apply in addition or in place of those listed in

Appendix A and the Appendix may be updated from time to time to include additional valid lawful basis.

- 4.2 In exercising a function under a valid lawful basis listed in Appendix A, or in accordance with Data Protection Legislation or any other applicable law, a Partner must have due regard to the guidance issued by the House of Bishops on safeguarding matters and must comply with the requirements of the Code. The applicable policies and guidance are listed in Appendix B.
- 4.3 There is an expectation that guidance and policies as referenced in paragraph 4.2 apply to all Partners, but to the extent that they do not a Partner should have applicable comparable policies in place (for example in the Channel Islands, the Isle of Man, countries that fall within the Diocese in Europe, the Church in Wales and Royal Peculiars).

4.4 Substantial Public Interest

- 4.4.1 The Substantial Public Interest conditions required by the UKGDPR and Data Protection Act 2018 are met by the aims and objectives listed in Section 2.
- 4.4.2 It is not always necessary or possible to obtain explicit consent for processing and sharing Special Category and Criminal Offence Data. Circumstances include:
- 4.4.2.1 where a crime may have been committed;
 - 4.4.2.2 where a person is judged to be at risk of significant/serious harm or a person is considered to be a risk of harm to themselves or others;
 - 4.4.2.3 The protective function of safeguarding would be prejudiced or prevented if a data subject withheld consent, for example in relation to:
 - investigations into allegations or circumstances surrounding allegations;
 - understanding what failures or mistakes had been made that led to a particular situation or event or series of events;
 - reviews which could result in recommendations for improved practice and the protection of individuals in the Church and engaged in Church activities.
- 4.4.3 Not obtaining consent does not alleviate any other duties or obligations with regard to processing Personal Data for safeguarding purposes. All processing:
- 4.4.3.1 must be recorded; and
 - 4.4.3.2 where appropriate, Data Subjects should be informed of the extent and nature of such processing.

4.4.4 Appropriate Policy document

- 4.4.4.1 Each Partner must have an appropriate policy document outlining compliance measures and retention policies for Special Category Data as required by the Data Protection Act 2018.
- 4.4.4.2 This requirement does not apply to non-UK data controllers e.g. Isle of Man, Jersey, Guernsey and the EU.

5.0 Data categories

- 5.1 The types of Personal Data, categories of Data Subjects and document and media types shared under this ISA are set out in Appendix A.

6.0 Specific Requirements and Restrictions

- 6.1 Personal Data shared between Partners must not be disclosed to any external body which is not a Signatory to this ISA without the written consent of the Providing Partner unless it has been requested by a statutory body (law enforcement, local authority, statutory enquiry, judicial review) or where necessary for the development, maintenance and support of IT systems. For the purposes of this ISA, approval for such sharing lies with the Nominated Individual of the Providing Partner.
- 6.2 All safeguarding information in the Church is currently under the legal hold imposed by the Independent Inquiry into Child Sexual Abuse (IICSA) and no destruction or disposal can take place until the legal hold is lifted. Such data may not be available for sharing if it would have been destroyed during the period of the legal hold i.e. should not be processed as its retention period has expired. Any data held by a Partner that is subject to this legal hold cannot be destroyed until the legal hold is lifted. The Lead Signatory will inform all partners when this happens, at which point the Church of England safeguarding retention schedule will apply.
- 6.3 In the circumstances where a case is referred to the NST and is being worked on jointly with the NST, or a case involves more than one Partner, each Partner is then responsible for ensuring the accuracy and quality of their record of the casework undertaken by that Partner. When a core group or safeguarding risk management meeting involves more than one Partner, and where any Partner in the core group or safeguarding risk management meeting may be required to collect and share information, that Partner is responsible for ensuring that such information is accurate and up to date.
- 6.4 Only appropriate and properly authorised persons should have access to the data specified in this ISA. An authorised person is someone with an office or role involved in safeguarding, e.g. diocesan or cathedral safeguarding advisors, communications officers, members of a diocesan safeguarding team, chair of a core group or safeguarding risk management meeting, chair of a safeguarding advisory panel, bishops, bishops' chaplains, deans, archdeacons, diocesan secretaries or deputy/assistant diocesan secretaries, diocesan registrars or other legal advisors;; members of the NST or a paid safeguarding advocate. Any local additions to this list should be agreed with the Nominated Individual who is responsible for ensuring appropriate access and use of shared information.
- 6.5 Data may be shared with internal IT or data officers or external contractors for the purposes of system development, maintenance and support as stated in Section 14 of the Framework.
- 6.6 Data may be shared with external legal advisors or insurers for the purposes of managing litigation, dispute resolution, judicial processes or insurance claims.

7.0 Core group or safeguarding risk management meeting

- 7.1 The purpose of the core group or safeguarding risk management meeting is to oversee and manage the response to a safeguarding concern or allegation in line with House of

Bishops' policy and practice guidance. Core group or safeguarding risk management meeting documents constitute shared Personal Data. However, disclosure outside the core group or safeguarding risk management meeting must be carefully considered, managed and controlled given the detrimental effect that disclosure may have on Data Subjects.

- 7.2 The sharing of core group or safeguarding risk management meeting minutes or documents to anyone who is not a participant of the group is only allowed on the written authorisation of the core group or safeguarding risk management meeting chair, or as specified in Section 1.6 of the practice guidance¹.
- 7.3 Where a Subject Rights Request is made that includes core group or safeguarding risk management meeting documents, these may have to be disclosed or amended, with appropriate redaction or notes only, and with the written consent of the core group or safeguarding risk management meeting Chair. Partners should take advice from their data protection leads.
- 7.4 Safeguarding risk assessments - A safeguarding risk assessment is commissioned and 'owned' by the Bishop. If the Bishop shares the document with an authorised individual (such as a DSA) or another Partner, those individuals or Partners should not share that risk assessment more widely without permission from the Bishop. Partners must take account of the Safeguarding (Clergy Risk Assessment) Regulations 2016 in particular regulations 4, 5, 6, and 7. The 2016 Regulations take precedence over the ISA.

8.0 Anonymised and Pseudonymised Information

- 8.1 The following Personal Data must be altered through aggregation or full anonymisation so that it is no longer Personal Data. While this type of data is no longer person-identifiable in theory, there is sometimes a risk that parts of a dataset could be de-anonymised, depending on the size of the involved group and how different datasets are combined. This means that care still needs to be taken in the treatment and management of this data and datasets to protect the privacy of individuals:
 - data reports to diocesan offices or the NST, governance bodies and governance panels;
 - practice reviews;
 - professional supervision case discussions and documents;
 - peer support case discussions and documents;
 - Serious Incident Reports (SIRs); and
 - any reports which will be published.
- 8.2 Information providers should decide whether requested data (if not listed above in 8.1) should be anonymised or pseudonymised to meet the Partner's requirements. Requesters should state whether they only require anonymised or pseudonymised information where this will be sufficient to meet their purpose.
- 8.3 A guide to appropriate anonymisation and pseudonymisation is provided separately. All Partners to this ISA will use appropriate techniques that ensure that recipients of shared data are unable to identify individual Data Subjects where relevant and/or necessary.

¹ Responding to, assessing and managing concerns or allegations against church officers practice guidance (2017): <https://www.churchofengland.org/sites/default/files/2017-12/Responding%20PG%20V2.pdf>

- 8.4 Care must be taken to prevent jigsaw or reverse engineered identification, i.e. the combining of other information about a Data Subject which makes them identifiable, even if their name has been removed.
- 8.5 Pseudonymised data is still Personal Data, e.g. where individuals are identifiable when combining different datasets or data elements. Partners should avoid using pseudonymisation where possible, and use anonymisation instead when seeking to remove identifiable data.
- 8.6 Data Subjects must not be named in the subject line of an email nor the title of documents where not strictly relevant or necessary.
- 8.7 If data is provided which has not been properly anonymised or pseudonymised, the Receiving Partner must contact the Providing Partner and delete/destroy the data provided. This may constitute a Data Breach and should be dealt with in accordance with the Framework.

9.0 Data Protection Impact Assessment (DPIA)

- 9.2 A DPIA has been carried out and approved by the Lead Signatory and the NCIs Data Protection Officer (NCIs DPO). A summary is provided at Appendix C.
- 9.3 All Partners must review the summary and take steps to put in place the relevant risk mitigations identified. If a Partner is unable to mitigate any risks, they must report this to the Lead Signatory and NCIs DPO.
- 9.4 The DPIA will be maintained by the Lead Signatory, and an annual review from the date this ISA comes into force will be undertaken and signed off by the NCIs DPO and shared with Partners. Any risks that arise during the period before the review should be reported to the Lead Signatory and will be assessed with the NCIs DPO and mitigation agreed with all Partners.

10.0 Signatures

- 10.1 By signing this agreement, all Signatories accept responsibility for its execution and agree to ensure that anyone handling shared data are sufficiently trained with regard to data protection so that requests for information and the process of sharing itself are sufficient to meet the purpose and requirements of this ISA.
- 10.2 Signatories must also ensure that they comply with all relevant legislation and with the provisions set out in the Church of England Information Sharing Framework.
- 10.3 A complete list of Signatories and signatures is attached at Appendix E.

Appendix A Lawful bases

Personal Data (Article 6)

UKGDPR	<p>Consent (Art 6(1)(a)) – for the sharing of data for the purpose of providing pastoral or therapeutic support; for requesting data from the police where consent is required; to share information from Pensions Board housing where required with local Diocesan Safeguarding teams.</p> <p>Legal obligation (Art 6(1)(c)):</p> <p>The Safeguarding and Clergy Discipline Measure 2016 Church of England Canon C30 “Of Safeguarding” Safeguarding (Clergy Risk Assessment) Regulations 2016 Safeguarding (Code of Practice) measure 2021:</p> <ul style="list-style-type: none">• Safeguarding in Religious Communities – effective from 17 May 2021• Declaration of Conflict of Interest Policy – effective from 8 November 2021• Safer Recruitment and People Management – effective from 4 January 2022• Safeguarding Learning and Development Framework – effective from 4 January 2022• Responding Well to Victims and Survivors of Abuse – effective from 4 April 2022• Safeguarding Children, Young People and Vulnerable Adults – effective from 4 July 2022 <p>Episcopal Endowments and Stipends Measure 1943 Chapter IX of the Constitution of the Church in Wales and the Clergy Terms of Service Canon 2010</p> <p>Vital interest (Art 6(1)(d)) – to protect someone from immediate risk where capacity to consent is lacking, or due to age/infirmity, or where there is the need to undertake investigations to protect individuals from immediate risk where the relationship with the respondent may prevent consent.</p> <p>Public task (Article 6(1)(e)):</p> <p>Church of England:</p> <p>House of Bishops’ Safeguarding Guidance (see Appendix B for details) Canon C30 “Of Safeguarding”; Safeguarding (Clergy Risk Assessment) Regulations 2016 Diocesan Safeguarding Advisors Regulations 2016; Canon C4 “Of the quality of such as are to be ordained deacons or priests” paragraph 2 (safer recruitment);</p>
--------	---

	<p>Canon C7 “Of examination of holy orders” – BAP process which requires sharing of information between DDO and Bishop and BAP</p> <p>Canon C8 “Of ministers exercising their ministry” paragraph 8, sub-para 1 and 2 – requirement to undertake training – allows for training completion to be checked and shared.</p> <p>Canon C10 “Of admission and institution” paragraph 2 (safer recruitment); paragraph 3(a) (safeguarding risk assessment/investigation);</p> <p>Canon C12 “Of the licensing of ministers under seal” paragraph 2 (provision of Clergy Current Status Letter and clergy personal files (commonly referred to as “clergy blue files”), which could include safeguarding data);</p> <p>Canon C18 “Of diocesan bishops” paragraphs 2 (jurisdiction); 3 (delegation of authority); 7(correction and punishment);</p> <p>Canon C26 “Of the manner of life of clerks in holy orders” paragraph 2 (applying safeguarding requirements);</p> <p>Canon E5 “Of the licensing of readers”;</p> <p>Canon E8 “Of the admission and licensing of lay workers”;</p> <p>The Churchwardens Measure 2001;</p> <p>The Church Representation Rules made under the Synodical Government Measure 1969.</p> <p>The Church of England Pension Measure 2018 Schedule 1, Part 2, (5)(1);</p> <ul style="list-style-type: none"> • The Church of England Pensions Board Safeguarding Policy and Guidance issued from time to time. <p>Multi-Agency Public Protection Arrangements (MAPPA Guidance Updated November 2021); Criminal Justice Act 2003.</p>
<p>Isle of Man - Data Protection (Application of GDPR) Order 2018;</p>	<p>Text of GDPR as applied to the Island in Annex to 2018 Order</p> <p>Consent (Art 6(1)(a)) – for the sharing of data for the purpose of providing pastoral or therapeutic support; for requesting data from the police where consent is required; to share information from Pensions Board housing where required with local Diocesan Safeguarding teams.</p> <p>Legal obligation (Art 6(1)(c))</p> <p>The Safeguarding and Clergy Discipline Measure (Isle of Man) 2017</p> <p>Church of England Canon C30 “Of Safeguarding”;</p> <p>Safeguarding (Clergy Risk Assessment) Regulations 2016</p> <p>Public task (Art 6(1)(e))</p> <p>House of Bishops’ Safeguarding Guidance (see Appendix B for details)</p>

	<p>Canon C30 “Of Safeguarding”; Safeguarding (Clergy Risk Assessment) Regulations 2016 Diocesan Safeguarding Advisors Regulations 2016;</p> <p>Canon C4 “Of the quality of such as are to be ordained deacons or priests” paragraph 2 (safer recruitment);</p> <p>Canon C7 “Of examination of holy orders” – BAP process which requires sharing of information between DDO and Bishop and BAP</p> <p>Canon C8 “Of ministers exercising their ministry” paragraph 8, sub-para 1 and 2 – requirement to undertake training – allows for training completion to be checked and shared.</p> <p>Canon C10 “Of admission and institution” paragraph 2 (safer recruitment); paragraph 3(a) (safeguarding risk assessment/investigation);</p> <p>Canon C12 “Of the licensing of ministers under seal” paragraph 2 (provision of Clergy Current Status Letter and clergy personal files (commonly referred to as “clergy blue files”), which could include safeguarding data);</p> <p>Canon C18 “Of diocesan bishops” paragraphs 2 (jurisdiction); 3 (delegation of authority); 7(correction and punishment);</p> <p>Canon C26 “Of the manner of life of clerks in holy orders” paragraph 2 (applying safeguarding requirements);</p> <p>Canon E5 “Of the licensing of readers”;</p> <p>Canon E8 “Of the admission and licensing of lay workers”;</p> <p>The Churchwardens Measure (Isle of Man) 2013</p>
The Data Protection (Jersey) Law 2018	
The Data Protection (Bailiwick of Guernsey) Law 2017	

Special Category Data (Article 9)

<p>UKGDPR</p> <p>Data Protection Act 2018</p>	<p>Explicit consent (Art 9(2)(a)) - for the sharing of data for the purpose of providing pastoral or therapeutic support; for requesting data from the police where consent is required; to share information from Pensions Board housing where required with local Diocesan Safeguarding teams.</p> <p>Vital interests (Art 9(2)(c)) - to protect someone from immediate risk where capacity to consent is lacking, e.g. due</p>
---	---

	<p>to age/infirmity, or where there is the need to undertake investigations to protect individuals from immediate risk where the relationship with the respondent may prevent consent.</p> <p>Legal claims (Art 9(2)(f)) - processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.</p> <p>Substantial Public interest (Art 9(2)(g)):</p> <p>Data Protection Act 2018 s. 10(3) and Schedule 1:</p> <ul style="list-style-type: none"> • Necessary for the exercise of a function conferred on a person by an enactment/rule of law (Schedule 1, Part 2 (6)) – sharing within the Church of England in order to provide information to e.g. an inquiry • Preventing or detecting unlawful acts (Schedule 1, Part 2 (10)) • Protection the public against dishonesty etc (Schedule 1, Part 2 (11)) • Safeguarding of children and individuals at risk (Schedule 1, Part 2 (18)) • Insurance (Schedule 1, Part 2 (20)) <p>Archiving, research and statistics (Art 9(2)(j))</p>
<p>Isle of Man - Data Protection (Application of GDPR) Order 2018</p> <p>Isle of Man- GDPR and LED Implementing Regulations 2018</p> <p>Isle of Man - Data Protection (Application of GDPR) Order 2018</p>	<p>Text of GDPR as applied to the Island in Annex to 2018 Order</p> <p>Legal claims (Art 9(2)(f))</p> <p>Substantial Public Interest (Art 9(2)(g)):-</p> <ul style="list-style-type: none"> • GDPR and LED Implementing Regulations 2018 reg. 12(3):- • Necessary for reasons of substantial public interest (Schedule 2, Part 2 (5) and Part 4 (30)):- • Necessary for the exercise of a function conferred on a person by an enactment (Schedule 2, Part 2 (6)); • Preventing or detecting unlawful acts (Schedule 2, Part 2 (8)); • Protecting the public against dishonesty etc. (Schedule 2, Part 2 (9)); • Safeguarding of children and natural persons at risk (Schedule 2, Part 2 (22)) <p>Archiving, research and statistics (Art 9(2)(j))</p>
<p>The Data Protection (Jersey) Law 2018</p>	
<p>The Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations 2018 (the “2018 Regulations”);</p>	

Criminal Offence Data (Article 10)

<p>UKGDPR Data Protection Act 2018</p>	<p>Data Protection Act 2018 s 10(5) and Schedule 1:-</p> <ul style="list-style-type: none"> • Necessary for the exercise of a function conferred on a person by an enactment/rule of law (Schedule 1, Part 2 (6)) • Preventing or detecting unlawful acts (Schedule 1, Part 2 (10)) • Protecting the public against dishonesty etc (Schedule 1, Part 2 (11)) • Safeguarding of children and individuals at risk (Schedule 1, Part 2 (18)) • Legal claims (Schedule 1, Part 3 (33)) • Extension of conditions in Part 2 of this Schedule referring to substantial public interest (Schedule 1, Part 3 (36))
<p>Isle of Man - Data Protection (Application of GDPR) Order 2018 Isle of Man - GDPR and LED Implementing Regulations 2018</p>	<p>Article 10</p> <ul style="list-style-type: none"> • GDPR and LED Implementing Regulations 2018 reg. 12(5):- • Public Interest (Schedule 2, Part 2 (5); Part 4 (30)) • Preventing or detecting unlawful acts (Schedule 2, Part 2 (8)); • Protecting the public against dishonesty etc. (Schedule 2, Part 2 (9))
<p>The Data Protection (Jersey) Law 2018</p>	
<p>The Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations 2018 (the "2018 Regulations")</p>	

Data categories

- Name
- Title
- Marital status
- Gender
- Nationality
- Job title/position
- Employment or work history
- Dates (birth, joined, ordination, education, death, licensed or commissioned etc)
- Contact information – work and personal (Address; phone numbers; email address)
- Honours
- Family names and biographical details, including wider family networks

- Lifestyle (including living conditions, daily habits, interests/hobbies, attitudes and behaviour and social circumstances)
- Family history details
- Previous and current safeguarding concerns
- Socio-economic details
- Employment and appointments
- Education and qualification details
- Training attendance/certification
- Housing needs
- Misconduct and unlawful acts e.g. the nature of any allegations
- Disqualification or suspension from office
- Funding relating to the provision of support

Special categories of information that may include:

- race
- ethnic origin
- religion
- health
- sex life or
- sexual orientation
- criminal allegations, proceedings or convictions, including DBS or other criminal records checks

Categories of people (includes current, former and prospective where relevant)

- Prospective, current, retired and former Church Officers (see definition)
- individuals involved in or connected with legal claims, inquiries, reviews and dispute resolution
- individuals who are supporting or advocating for victims or survivors
- individuals who are supporting or advocating for those responding to allegations of abuse or misconduct
- professional advisers and consultants
- individuals whose safety has been / alleged to have been put at risk
- children and parents/ carers
- individuals who are the subject of complaints of misconduct and/or unlawful acts
- individuals who may pose a risk

Document and media types

- records of alerts, concerns or allegations;
- case files;
- risk assessments;
- safeguarding agreements;

- confidential declaration forms;
- recruitment and appointment documentation e.g. DBS or other criminal record checks; proof of identity;
- training and professional development records;
- referrals;
- self-referrals;
- minutes of meetings;
- correspondence, including letters, emails etc.;
- notes from telephone conversations;
- records of enquiries, advice sought or provided;
- records provided by the police or statutory agencies;
- Learning Lesson Reviews (LLRs) or other Review documents and reports;
- disciplinary records relating to safeguarding;
- notifications to external parties e.g. Charity Commission, insurers etc.;
- images and audio such as photographs, CCTV or other images, recordings of remote meetings via video calls (e.g. Zoom, Teams), either audio only, or audio and video;
- statement and records of support as defined in Section 5 of “Responding Well to Victims and Survivors of Abuse”
- apologies and related documents (lessons learnt, notes of reconciliation meetings etc)

Appendix B Policies

Section A - Church of England Safeguarding Policies and Guidance

Changes to the law made by the Safeguarding (Code of Practice) Measure 2021

The Safeguarding (Code of Practice) Measure 2021 (the **2021 Measure**) replaces and strengthens the duty to have due regard to House of Bishops' safeguarding guidance with a duty to comply with the requirements in a new safeguarding code of practice (the **Code**).

The status of the existing safeguarding guidance

Each piece of House of Bishops' safeguarding guidance that is in place on 1 March 2022 remains in place until that guidance is replaced by a Code of Practice. In order for any part of the Code to be adopted, it must first undergo the consultation and approval processes set out in the 2021 Measure.

All of the existing House of Bishops' Safeguarding Guidance is currently available from the Church of England Safeguarding Policy and Guidance page. [Policy and practice guidance | The Church of England](#)

A new e-manual is being created which will, in due course, have the new Code and any Guidance in force uploaded onto it. [Safeguarding e-manual | The Church of England](#)

Revised guidance	Effective Date
Safeguarding in Religious Communities	17 th May 2021
Declaration of Conflict of Interest Policy	8 th Nov 2021
Safer Recruitment and People Management	4 th Jan 2022
Safeguarding Learning and Development Framework	4 th Jan 2022
Responding Well to Victims and Survivors of Abuse	4 th April 2022
Safeguarding Children, Young People and Vulnerable Adults	4 th July 2022

Section B - Church of England "Blue File" policy

[Personal Files Relating to Clergy](#)

Section C - Church in Wales

- Disciplinary Offences as follows in Chapter IX of the Constitution:
 - 1.1. Wilful disobedience to or breach of any of the provisions of the Constitution or of the Statement of Terms of Service published pursuant to the Clergy Terms of Service Canon 2010;
 - 1.2. Failure to comply with advice from the Provincial Safeguarding Panel without reasonable excuse.
- [Church in Wales Clergy Personal Files Policy](#)
- Church in Wales Privacy Notice: <https://www.churchinwales.org.uk/en/privacy-notice/>

Appendix C Data Protection Impact Assessment

Section 4 – Review and Sign-Off

(A copy of the full DPIA can be obtained on request to the NCIs Data Protection Officer)

Final Project Risk Rating (Tick relevant box)

Note: In the event of one or more the residual risks being identified as high, then this will automatically rate the whole project as a high risk.

Risk level	Action	Tick here
Low Risk (2-6)	Project can proceed	
Medium Risk (8)	Minor actions are required before proceeding	x
High Risk (12 -16)	Significant actions required may need to be submitted to the ICO for evaluation	

NCIs DPO comments

Although there are overall risk rating is medium, there are a number of mitigations required from all Partner organisation to achieve this risk level. Partner Organisations must take responsibility for ensuring that they are compliant with the requirements of Information Sharing as outlined in the ISA, and to undertaking the necessary actions to mitigate risks in their organisations.

If there any risks that cannot be mitigated this must be brought to the attention of the Lead Signatory.

Required Mitigations

#	Required Mitigation to achieve residual risk
1	Finalisation of the ISA, and Partner Organisations signing up to it.
2	Finalisations and publication of the HR Information Sharing Privacy Notice
3	Partner organisations should review their data protection arrangements and find pragmatic solutions for what could be a limited requirement.
4	Partner organisations should train their staff on keeping data secure and ensure all storage repositories, including for paper storage, are secure and only accessed by authorised individuals
5	At the time data sharing is required, each partner organisation must look to use the safest method of sharing that they have access to or ensure that they provide suitably secure methods using appropriate software or applications and train their staff to use them.
6	Each Partner Organisation should ensure that they have the appropriate controls in place to share information, and that the Partner Organisation that they are planning to share data with has equally appropriate controls in place for protecting the data being shared
7	Partners will receive additional training on data sharing, core groups will be reminded about what data sharing controls apply.
8	All Partners to monitor changes in practice or process and inform the Lead Signatory. The NCIs DPO and the CoE DPO network will monitor changes in the law. Updates will be issued to all partners when necessary.

9	All Partner organisation to ensure that the documents and agreements are shared with relevant individuals and that appropriate handover is done if senior officers leave the organisation; the NCIs will inform the HR, DSA, DPO and Communications networks.
10	NCIs to clarify the use of consent for data processing in Safeguarding Policy and Practice guidance; advice to be provided by data protection leads/DPO's in Partner Organisations

Review - Sign Off


Position	Name	Date
Information Sharing Project Senior Responsible Officer	Nathalie Ballard	08/02/2022
Safeguarding Casework Team Manager	Ian Bowles	21/01/2022
NCIs Data Protection Officer	Madi McAllister	19/01/22

Authorisation Levels

The DPIA must be signed off in Section 4 by the following roles according to the assigned risk level:

High Risk	Senior Information Risk Owner (SIRO) or in cases where Risks cannot be mitigated submitted to ICO for review or the project is terminated.
Low and Medium risk	Information Asset Owner(s) or Project Manager

DPIA – Approval and Final Sign Off

Position	Name	Signature	Date
Interim Director of Safeguarding (Lead Signatory)	Zena Marshall		09/02/22

Safeguarding Information Sharing - Privacy Notice

This privacy notice is provided to explain what to expect when we share your personal information in accordance with the UK GDPR and Data Protection Act 2018, the EU GDPR, and relevant data protection legislation in the Isle of Man, Jersey and Guernsey and the Channel Islands.

1. Data controller

The Data Controllers are the Partner Organisations that have signed up to the Safeguarding Information Sharing Agreement. This list is regularly revised to ensure that it is up to date. To obtain a full list please contact the relevant Data Controller using the contact details in Section 8 below.

2. Why we share your personal data:

Personal information is shared for the following purposes:

- 2.1 Promoting and maintaining a safer culture within the Church that protects and promotes the welfare of children, young people and vulnerable adults as required by "Promoting a Safer Church";
- 2.2 creating and maintaining environments that are safer for all, that promote well-being, that prevent abuse, and that create nurturing, caring conditions within the Church for children, young people and vulnerable adults and help identify people who may pose a risk to others and, where possible, work to reduce offending behaviour;
- 2.3 to enable the Pensions Board housing service to put in place safeguarding risk management or support arrangements (with other agencies and Diocesan safeguarding teams as necessary);
- 2.4 to enable Pensions Board housing to support other agencies in carrying out their statutory functions (e.g. prevention of crime), including the need to process criminal offence data to ensure we house you appropriately if you are currently under supervision of a statutory authority.
- 2.5 preventing death or serious harm;
- 2.6 the safer recruitment of all those with any responsibility in a Partner organisation relating to children, young people and vulnerable adults within the Church;
- 2.7 training and equipping Church Officers to have the confidence and skills they need to care for and support children, young people and vulnerable adults including recognising and responding to abuse and identifying low-level concerns that may reveal people at risk of abuse;
- 2.8 responding to every safeguarding concern or allegation appropriately and recording all safeguarding work; coordinating effective and efficient responses and preventing abuse and harm that may increase the need for care and support;
- 2.9 reporting all suspicions, concerns, knowledge or allegations, that reach the relevant threshold, to the appropriate statutory authorities irrespective of the status of the person;
- 2.10 offering care and support to all those who are known to have been abused or allege abuse, or are considered to be vulnerable to abuse regardless of the type of abuse, when or where it occurred and to help people access support to reduce risk and

promote wellbeing, including making a suitable apology when required or considered necessary;

- 2.11 offering care and support to all those who are the subject of safeguarding allegations or investigations and help people to access support to reduce risk and promote wellbeing;
- 2.12 taking responsibility for ensuring that steps are taken to protect others when any Church Officer and any individual regularly involved with a Church body is considered a risk to children, young people and vulnerable adults and enabling early interventions to prevent the escalation of risk;
- 2.13 working to mitigate any identified risks in collaboration with the relevant statutory agencies in accordance with relevant law;
- 2.14 providing professional supervision by the National Safeguarding Team to persons with operational responsibility for safeguarding in Partner organisations;
- 2.15 providing reports to local, national or statutory bodies responsible for oversight of safeguarding within Partners;
- 2.16 liaison with internal and external advisers for the purpose of litigation, dispute resolution, judicial process or or to process information related to an insurance claim;
- 2.17 providing anonymised Serious Incident Reports to the National Safeguarding Team;
- 2.18 undertaking investigations and reviews (including lessons learnt reviews) and engaging in peer support to maintain and improve good practice in safeguarding; understanding failings in particular cases or safeguarding practice; improving processes and case management and revealing patterns of abuse that were previously undetected and that could identify others at risk of abuse;;
- 2.19 maintaining accurate and up to date information on: Disclosure and Barring Service (DBS) checks; training and post/positions held by anyone within a Partner organisation with any responsibility relating to children, young people and vulnerable adults;
- 2.20 research purposes in order to quality assure safeguarding practice and inform strategic planning on safeguarding for example the conduct of lessons learnt reviews.

3. The categories of personal data we collect:

The information we share for this these purposes may include:

- Name
- Title
- Marital status
- Gender
- Nationality
- Job title/position
- Employment or work history
- Dates (birth, joined, ordination, education, death, licensed or commissioned etc)
- Contact information – work and personal (addresses; phone numbers; email addresses)
- Honours
- Family names and biographical details, including wider family networks

- Lifestyle (including living conditions, daily habits, interests/hobbies, attitudes and behaviour and social circumstances)
- Family history details
- Previous and current safeguarding concerns
- Socio-economic details
- Employment and appointments
- Education and qualification details
- Training attendance/certification
- Housing needs
- Misconduct and unlawful acts e.g. the nature of any allegations
- Disqualification or suspension from office
- Funding relating to the provision of support

We also process “special categories” of information that may include:

- race;
- ethnic origin;
- religion;
- health;
- sex life or
- sexual orientation.

In addition we will process criminal offence data where required:

- criminal allegations, proceedings or convictions, including DBS or other criminal records checks

4. The lawful basis for using your information:

We collect and use personal data under the following lawful bases:

4.1 Personal data (see Section 2 above)

UKGDPR	<p>Consent (Art 6(1)(a)) – for the sharing of data for the purpose of providing pastoral or therapeutic support; for requesting data from the police where consent is required; to share information from Pensions Board housing where required with local Diocesan Safeguarding teams.</p> <p>Legal obligation (Art 6(1)(c)):</p> <ul style="list-style-type: none"> • The Safeguarding and Clergy Discipline Measure 2016 • Church of England Canon C30 “Of Safeguarding” • Safeguarding (Clergy Risk Assessment) Regulations 2016 • Safeguarding (Code of Practice) measure 2021: • Safeguarding in Religious Communities – effective from 17 May 2021 • Declaration of Conflict of Interest Policy – effective from 8 November 2021 • Safer Recruitment and People Management – effective from 4 January 2022
--------	--

- Safeguarding Learning and Development Framework – effective from 4 January 2022
- Responding Well to Victims and Survivors of Abuse – effective from 4 April 2022
- Safeguarding Children, Young People and Vulnerable Adults – effective from 4 July 2022
- Episcopal Endowments and Stipends Measure 1943
- Chapter IX of the Constitution of the Church in Wales and the Clergy Terms of Service Canon 2010

Public task (Article 6(1)(e)):

Church of England:

- House of Bishops' Safeguarding Guidance (see Appendix B for details)
- Canon C30 "Of Safeguarding";
- Safeguarding (Clergy Risk Assessment) Regulations 2016
- Diocesan Safeguarding Advisors Regulations 2016;
- Canon C4 "Of the quality of such as are to be ordained deacons or priests" paragraph 2 (safer recruitment);
- Canon C7 "Of examination of holy orders" – BAP process which requires sharing of information between DDO and Bishop and BAP
- Canon C8 "Of ministers exercising their ministry" paragraph 8, sub-para 1 and 2 – requirement to undertake training – allows for training completion to be checked and shared.
- Canon C10 "Of admission and institution" paragraph 2 (safer recruitment); paragraph 3(a) (safeguarding risk assessment/investigation);
- Canon C12 "Of the licensing of ministers under seal" paragraph 2 (provision of Clergy Current Status Letter and clergy personal files (commonly referred to as "clergy blue files"), which could include safeguarding data);
- Canon C18 "Of diocesan bishops" paragraphs 2 (jurisdiction); 3 (delegation of authority); 7(correction and punishment);
- Canon C26 "Of the manner of life of clerks in holy orders" paragraph 2 (applying safeguarding requirements);
- Canon E5 "Of the licensing of readers";
- Canon E8 "Of the admission and licensing of lay workers";
- The Churchwardens Measure 2001;
- The Church Representation Rules made under the Synodical Government Measure 1969.
- The Church of England Pension Measure 2018 Schedule 1, Part 2, (5)(1);
 - The Church of England Pensions Board Safeguarding Policy and Guidance issued from time to time.
- Multi-Agency Public Protection Arrangements (MAPPA Guidance Updated November 2021); Criminal Justice Act 2003.

Vital interest (Art 6(1)(d)) – to protect someone from immediate risk where capacity to consent is lacking, or due to age/infirmity, or where there is the need to undertake investigations to protect individuals from immediate risk where the relationship with the respondent may prevent consent.

<p>Isle of Man - Data Protection (Application of GDPR) Order 2018;</p>	<p>Text of GDPR as applied to the Island in Annex to 2018 Order</p> <p>Consent (Art 6(1)(a)) – for the sharing of data for the purpose of providing pastoral or therapeutic support; for requesting data from the police where consent is required; to share information from Pensions Board housing where required with local Diocesan Safeguarding teams.</p> <p>Legal obligation (Art 6(1)(c))</p> <ul style="list-style-type: none"> • The Safeguarding and Clergy Discipline Measure (Isle of Man) 2017 • Church of England Canon C30 “Of Safeguarding”; • Safeguarding (Clergy Risk Assessment) Regulations 2016 <p>Public task (Art 6(1)(e))</p> <ul style="list-style-type: none"> • House of Bishops’ Safeguarding Guidance (see Appendix B for details) • Canon C30 “Of Safeguarding”; • Safeguarding (Clergy Risk Assessment) Regulations 2016 • Diocesan Safeguarding Advisors Regulations 2016; • Canon C4 “Of the quality of such as are to be ordained deacons or priests” paragraph 2 (safer recruitment); • Canon C7 “Of examination of holy orders” – BAP process which requires sharing of information between DDO and Bishop and BAP • Canon C8 “Of ministers exercising their ministry” paragraph 8, sub-para 1 and 2 – requirement to undertake training – allows for training completion to be checked and shared. • Canon C10 “Of admission and institution” paragraph 2 (safer recruitment); paragraph 3(a) (safeguarding risk assessment/investigation); • Canon C12 “Of the licensing of ministers under seal” paragraph 2 (provision of Clergy Current Status Letter and clergy personal files (commonly referred to as “clergy blue files”), which could include safeguarding data); • Canon C18 “Of diocesan bishops” paragraphs 2 (jurisdiction); 3 (delegation of authority); 7(correction and punishment); • Canon C26 “Of the manner of life of clerks in holy orders” paragraph 2 (applying safeguarding requirements); • Canon E5 “Of the licensing of readers”; • Canon E8 “Of the admission and licensing of lay workers”; • The Churchwardens Measure (Isle of Man) 2013
--	---

4.2 Special category data (see Section 2 above)

<p>UKGDPR Data Protection Act 2018</p>	<p>Explicit consent (Art 9(2)(a)) - for the sharing of data for the purpose of providing pastoral or therapeutic support; for requesting data from the police where consent is required.</p> <p>Vital interests (Art 9(2)(c)) - to protect someone from immediate risk where capacity to consent is lacking, e.g. due to age/infirmity, or where there is the need to undertake investigations to protect individuals from immediate risk where the relationship with the respondent may prevent consent.</p>
--	---

	<p>Legal claims (Art 9(2)(f)) - processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.</p> <p>Substantial Public interest (Art 9(2)(g)):</p> <p>Data Protection Act 2018 s. 10(3) and Schedule 1:</p> <ul style="list-style-type: none"> • Necessary for the exercise of a function conferred on a person by an enactment/rule of law (Schedule 1, Part 2 (6)) – sharing within the Church of England in order to provide information to e.g. an inquiry • Preventing or detecting unlawful acts (Schedule 1, Part 2 (10)) • Protection the public against dishonesty etc (Schedule 1, Part 2 (11)) • Safeguarding of children and individuals at risk (Schedule 1, Part 2 (18)) • Insurance (Schedule 1, Part 2 (20)) <p>Archiving, research and statistics (Art 9(2)(j))</p>
<p>Isle of Man - Data Protection (Application of GDPR) Order 2018</p> <p>Isle of Man- GDPR and LED Implementing Regulations 2018</p> <p>Isle of Man - Data Protection (Application of GDPR) Order 2018</p>	<p>Text of GDPR as applied to the Island in Annex to 2018 Order</p> <p>Legal claims (Art 9(2)(f))</p> <p>Substantial Public Interest (Art 9(2)(g)):-</p> <ul style="list-style-type: none"> • GDPR and LED Implementing Regulations 2018 reg. 12(3):- • Necessary for reasons of substantial public interest (Schedule 2, Part 2 (5) and Part 4 (30)):- • Necessary for the exercise of a function conferred on a person by an enactment (Schedule 2, Part 2 (6)); • Preventing or detecting unlawful acts (Schedule 2, Part 2 (8)); • Protecting the public against dishonesty etc. (Schedule 2, Part 2 (9)); • Safeguarding of children and natural persons at risk (Schedule 2, Part 2 (22)); <p>Archiving, research and statistics (Art 9(2)(j))</p>

4.3 Criminal Offence data

<p>UKGDPR</p> <p>Data Protection Act 2018</p>	<p>Data Protection Act 2018 s 10(5)and Schedule 1:-</p> <ul style="list-style-type: none"> • Necessary for the exercise of a function conferred on a person by an enactment/rule of law (Schedule 1, Part 2 (6)) • Preventing or detecting unlawful acts (Schedule 1, Part 2 (10)) • Protecting the public against dishonesty etc (Schedule 1, Part 2 (11)) • Safeguarding of children and individuals at risk (Schedule 1, Part 2 (18)) • Legal claims (Schedule 1, Part 3 (33)) • Extension of conditions in Part 2 of this Schedule referring to substantial public interest (Schedule 1, Part 3 (36))
<p>Isle of Man - Data Protection (Application of GDPR) Order 2018</p>	<p>Article 10</p> <ul style="list-style-type: none"> • GDPR and LED Implementing Regulations 2018 reg. 12(5):- • Public Interest (Schedule 2, Part 2 (5); Part 4 (30)) • Preventing or detecting unlawful acts (Schedule 2, Part 2 (8));

Isle of Man - GDPR and LED Implementing Regulations 2018	<ul style="list-style-type: none"> • Protecting the public against dishonesty etc. (Schedule 2, Part 2 (9))
--	--

5. Who we collect from or share your information with:

We collect your information from:

- You (the Data Subject)
- Church of England records
- Partner Organisations

6. Your data will be transferred outside the UK

Your personal data once received may be transferred between the Isle of Man, Jersey, Guernsey and the European Union, and is protected by adequacy arrangements with those jurisdictions.

7. How long do we keep your information?

The information will be retained in accordance with the purpose for which it is used, please contact the relevant Partner Organisation to obtain a copy of their retention schedule.

8. Your rights:

You have the following rights regarding your personal data:

- The right to be informed about any data we hold about you;
- The right to request a copy of your personal data which we hold about you;
- The right to withdraw your consent at any time (if applicable);
- The right to request that we correct any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for us to retain such data;
- 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;
- The right to object to the processing of your personal data (if applicable);
- The right to obtain and reuse your personal data to move, copy or transfer it from one IT system to another (if applicable).

To exercise these rights, please contact the data controller using the contact information provided below.

9. Complaints or concerns:

If you have any queries regarding the data sharing please contact the relevant data controller using the contact information below.

<insert email address and other contact details>

You have the right to make a complaint at any time to:

UK - Information Commissioner's Office (ICO) online at:

[Your personal information concerns | ICO](#), or by phone on 0303 123 1113 (local rate).

Sodor & Man - refer to Isle of Man Information Commissioner 01624 693 260

<insert details for Jersey, Guernsey, Brussels>

Appendix E Signatures

Lead Signatory – Zena Marshall, Interim Director of Safeguarding, National Safeguarding Team, Archbishops' Council

A handwritten signature in black ink, appearing to read 'Z Marshall', followed by a period.

