APPROPRIATE POLICY DOCUMENT

1. About this policy

1.1 This is the "appropriate policy document" for the Catholic Safeguarding Advisory Service ('CSAS'Ss) setting out how we will handle and protect special categories of personal data and criminal convictions data. CSAS is an agency of the Catholic Trust for England and Wales ('CaTEW') and so this policy should be read alongside CaTEW's Data Protection Policy and record of processing activities.

1.2 This document meets the requirement of the Data Protection Act 2018 that an appropriate policy document be in place where processing special categories of personal data and criminal convictions data in certain circumstances.

2. Definitions

Controller: the person or organisation that determines when, why and how to process Personal Data.

Criminal convictions data: personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.

Data Retention Policy: explains how the organisation classifies and manages the retention and disposal of its information. Time periods for retention are set out in the Data Retention Policy.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Impact Assessment (DPIA): an assessment used to identify and reduce risks of a data processing activity.

DPA 2018: the Data Protection Act 2018.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR.

GDPR: the General Data Protection Regulation (*(EU) 2016/679*).

Personal data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably possess. Personal Data includes special categories of personal data.

Privacy Notice: a separate notice setting out information that must be provided to Data Subjects when the organisation collects information about them.

Processing or **process**: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data

including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special categories of personal data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

3. Why CSAS processes special categories of personal data and criminal convictions data

3.1 CSAS processes special categories of personal data and criminal convictions data for the following purposes:

(a) [checking applicants' and employees' right to work in the UK and verifying that candidates are suitable for employment or continued employment] on behalf of the dioceses and religious congregations in respect of DBS processing;

(b) meeting our obligations to share personal data for safeguarding purposes; and

(c) to provide an advisory service, quality assurance processes and to support diocesan and religious congregation safeguarding processes

4. Data protection principles

4.1 The GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

4.2 CaTEW and CSAS comply with the principles relating to the processing of personal data set out in the GDPR which require personal data to be:

(a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation); and

(f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Integrity and Confidentiality).

4.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Compliance with the data protection principles

<u>Lawfulness, fairness and transparency</u>

5.1 CSAS will process personal data fairly and lawfully and only for specified purposes. We will process special categories of personal data and criminal convictions data only if we have a legal ground for processing and one of the specific processing conditions relating to special categories of personal data or criminal convictions data applies. We will identify and document the legal ground and specific processing condition relied on for each processing activity.

5.2 When collecting special categories of personal data and criminal convictions data, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), CSAS will provide Data Subjects with a Privacy Notice setting out all the information required by the GDPR. CSAS's privacy notice is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood. The lawful bases we rely on are set out in the table below:

Article 6 lawful basis for processing	**Article 9 lawful basis for processing special categories of personal data**
Data relating to safeguarding (this may include criminal convictions data, health data, or any other type of special categories of personal data which is processed for safeguarding purposes) Compliance with a legal obligation (*Article 6 (1)(c)*) or in our legitimate interests (*Article 6(1)(f)*) which are not outweighed by the fundamental rights and freedoms of the Data Subject.	Necessary to protect vital interests of the Data Subject where they are incapable of giving consent (*Article 9(2)(c)*). Necessary for the establishment, exercise or defence of legal claims (*Article 9(2)(f)*). Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018, such as preventing or detecting unlawful acts (*paragraph 10(1), Schedule 1, DPA 2018*).
Criminal convictions data Compliance with a legal obligation (*Article 6(1)(c)*) or in our legitimate interests (*Article 6(1)(f)*) which are not outweighed by the fundamental rights and freedoms of the Data Subject.	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with employment, social security or social protection (*paragraph 1(1)(a), Schedule 1, DPA 2018*). Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018, such as preventing or detecting unlawful acts (*paragraph 10(1), Schedule 1, DPA 2018*).

<u>Purpose limitation</u>

5.3 CSAS will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in our Privacy Notice.

Data minimisation

5.4 CSAS will only collect or disclose the minimum personal data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the personal data collected is adequate and relevant for the intended purposes.

Accuracy

5.5 CSAS will ensure that the personal data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Storage limitation

5.6 CSAS only keeps personal data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

5.7 CSAS maintains a Data Retention Policy to ensure personal data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

5.8 CSAS will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Integrity and confidentiality

5.9 CaTEW and CSAS will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data.

Accountability

5.10 CaTEW is responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the CaTEW DPO.

5.11 CaTEW will:

(a) Ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request.

(b) Carry out a DPIA for any high-risk processing of personal data to understand how processing may affect Data Subjects and consult the Information Commissioner if necessary.

(c) Ensure that a DPO is appointed to provide independent advice and monitoring of personal data handling, and that the DPO has access to report to the highest management level.

(d) Have internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.

6. Controller's policies on retention and erasure of personal data

6.1 CaTEW takes the security of special categories of personal data and criminal convictions data very seriously. We have administrative, physical and technical safeguards in place to protect personal data against unlawful or unauthorised processing, or accidental loss or damage. We will ensure, where special categories of personal data or criminal convictions data are processed that:

(a) The processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy.

(b) Where we no longer require special categories of personal data or criminal convictions data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

(c) Where records are destroyed we will ensure that they are safely and permanently deleted.

6.2 Data Subjects receive a Privacy Notice setting out how their personal data will be handled when we first obtain their personal data, and this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

7. Review

7.1 This policy on processing special categories of personal data and criminal convictions data is reviewed at least every two years or in accordance with any changes in legislation if sooner.

7.2 The policy will be retained where CSAS process special categories of personal data and criminal convictions data and for a period of at least six months after we stop carrying out such processing.

7.3 A copy of this policy will be provided to the Information Commissioner on request.