CSAS Information Security Policy for Disclosure and Barring Checking Services
Including Handling, Access, Usage, Storage, Retention & Disposal
of Disclosures & Disclosure Information

As an organisation using the Disclosure and Barring Service (DBS) to help assess the suitability of applicants for positions of trust, CSAS complies fully with the **DBS Code of Practice** regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. It also complies fully with its obligations under the **Data Protection Act** and other relevant legislation.

Information Security is a recurring agenda item at Safeguarding Coordinator meetings

For the purpose of this policy CSAS includes its agents within the safeguarding structure of the Catholic Church of England & Wales who process Disclosure Applications and may hold information relating to that processing locally, within the relevant Diocese.

1. Objectives of the Information Security Policy

- Information is afforded adequate protection in accordance with its sensitivity. It is recognised that information about criminal proceedings constitutes sensitive personal data and as such attracts an enhanced level of protection under the **Data Protection Act.**
- Information held can be relied upon for completeness and accuracy.
- Information is used, maintained, stored and disposed of in compliance with all applicable laws, regulations and contractual obligations.
- Access to information and associated IT systems only permitted to persons who have a business need for such access and such access is restricted to the purposes associated with their role.
- Any processing of personal data will be carried out in accordance with the provisions of the **Data Protection Act**.

2. Classification

CSAS regards Disclosures and Disclosure information as confidential and requires that this policy is adhered to in relation to that information. As such that information must be treated as confidential and therefore stored securely and only accessed by individuals who need to know the content. When no longer required that information must be securely destroyed. Confidential documentation must not be stored on unsecure shared network drives or mobile devices. Care should be taken when verbally discussing confidential information whilst in public places, in relation to messages left on answering machines and in electronic communications. Information transmitted verbally or electronically should be subject to the same level of protection as physical documents so as to ensure the confidentiality, security and integrity of the information.

3. Handling and Access

In accordance with Section 124 of the Police Act 1997 (as amended), Disclosure information must only be passed on to those who are authorised to receive it in the course of their duties. CSAS maintains a record of all those to whom Disclosures or Disclosure information has been disclosed and recognises that it is a criminal offence to pass this information on to anyone who is not entitled to receive it.

Only named individuals, having signed the CSAS DBS Confidentiality Agreement and received appropriate training, are permitted access to Disclosure documentation / to process applications / to carry out the ID verification process.

All applications to DBS must be counter-signed. Counter-signatories are chosen by the CSAS Lead Counter-signatory and cannot countersign applications until they have undertaken mandatory counter-signatory training and signed the CSAS DBS Confidentiality Agreement.

E-Bulk users will be set up with the correct permissions according to the user's designated role of Master Disclosure Manager, Disclosure Manager or ID Verifier and appropriate training will be provided. Master Disclosure Managers and Disclosure Managers will be required to sign the CSAS e-Bulk End User Agreement before access to the system is granted.

Access to Disclosure e-Bulk schema results is limited to Master Disclosure Managers and Disclosure Managers. ID Verifiers will not have access to e-Bulk schema results or be able to export information.

Only the e-Bulk service provider shall have access to the e-Bulk system for the purposes of maintenance and upgrade. Third party requests for access to the system will need to be approved by the Facilities and Operations Manager (via CSAS), who acts as the gateway for all information security requests, which are dealt with in accordance with this policy and all other relevant policies and procedures. Third parties who are granted access to information to which this policy applies will be required to sign the CSAS DBS Confidentiality Form before access is granted. Their access will be the minimum required for the duration to carry out the task requested of them.

The DBS may, during the course of provisioning Registered Bodies to use the eBulk service, provide access to, or enable them to acquire knowledge of, the DBS's technical and process specifications, systems, and other information of or with respect to security and technical measures which may not be accessible or known to the general public. Such information must be protected from inappropriate access and unauthorised disclosure. Any requests for disclosure information relating to e-Bulk, including any made under the Freedom of Information Act should be referred to CSAS (for referral to the DBS) before disclosure is considered. Requests for the release of any documentation issued by the DBS and classified as "restricted" must not be disclosed by anyone other than the DBS.

4. Usage

Disclosure information must only be used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

5. Storage and Retention

Disclosure information must not be kept on an applicant's personnel file and must always be kept separately and securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are authorised to see it as part of their duties.

Once a recruitment (or other relevant) decision has been made, CSAS do not keep Disclosure information for any longer than is absolutely necessary. This is generally for a period of up to 6 months, to allow for the consideration and resolution of any disputes or complaints. If it is considered necessary to keep Disclosure information for longer than 6 months, we will consult the DBS and give full consideration to the rights of the data subject under the Data Protection Act 1998 and the Human Rights Act 1998 before doing. Throughout this time, the requirements set out above regarding the safe storage and strictly controlled access will continue to apply. Any retention beyond 6 months will be limited to the minimum period necessary.

CSAS must not make or keep any copy or representation of the contents of a Disclosure. CSAS will however keep a record of the date of issue of a Disclosure, the name of the data subject, the type of the Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

E-Bulk schema results are not to be printed out, nor retained electronically other than within the e-Bulk system. The e-Bulk system will automatically retain information for a period of 6 months following a Disclosure result.

6. Disposal

Once the retention period has elapsed, CSAS ensure that any Disclosure information is permanently and securely destroyed when no longer needed by dust shredding machines (or other equally destructive method) so it is not readable/useable for any purpose. While awaiting destruction, Disclosure information must not be kept in any unsecure receptacle (e.g. waste bin or confidential waste sack).

The e-Bulk system will automatically purge the Disclosure information and any supporting information (such as ID verification) after 6 months.

7. Acting as an Umbrella Body

Before acting as an Umbrella Body (one which counter-signs applications and receives Disclosure information on behalf of other employers or recruiting organisations connected to the Catholic

Community in England and Wales,) CSAS will take all reasonable steps to satisfy ourselves that the organisations that we act as an Umbrella Body for will handle, use, store, retain and dispose of Disclosure information in full compliance with the DBS Code of Practice and in full accordance with this policy. We will also ensure that any organisation or individual, at whose request applications for Disclosure are countersigned, has such a written policy and if necessary will provide a model policy to use or adapt for this purpose.