Catholic Safeguarding Standards Agency

Building trust, delivering change.

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

## Policy statement

As an organisation using the Disclosure and Barring Service (DBS) to help assess the suitability of applicants for positions working with children, young people and adults at risk, CSSA 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 General Data Protection Regulation 2016 and the Data Protection Act 2018 and other relevant legislation.

This policy applies to CSSA and its agents within the safeguarding structures of dioceses and religious congregations, across the Catholic Church of England and Wales, who process Disclosure Applications and may hold information relating to that processing locally.

All DBS applicants using the CSSA registered body will be issued with a DBS specific Privacy Notice and will be required to sign an application form in relation to the processing of their application agreeing to the use of their personal information for the DBS check.

## 1. Objectives of the Information Security Policy

To ensure that:

- DBS related information is afforded adequate protection in accordance with its sensitivity. It is recognised that information about criminal proceedings is not permitted to be processed under the General Data Protection Regulation unless UK domestic law permits processing. UK domestic law allows for processing of this information in certain circumstances within 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 is 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 General Data Protection Regulation and the Data Protection Act.

## 2. Classification

CSSA regards Disclosures and Disclosure information as confidential and requires that agents of the Registered Body adhere to the requirements set out in this policy document.

Disclosures and Disclosure related must be stored securely and only accessed by individuals who need to know the content.

Information transmitted verbally or electronically should be subject to the same level of protection as physical documents to ensure the confidentiality, security and integrity of the information. Confidential documentation must not be stored on unsecured shared network drives or mobile devices. Confidential information should not be discussed in public places and confidential or sensitive information should not be left on answerphone messages. When transmitting Disclosure related information electronically e.g. via email, documents should be encrypted and confidential information should not be included in the subject line or body of the email text.

When no longer required, Disclosure related e information must be securely destroyed in accordance with the timescales set out in the record retention schedule.

**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. CSSA 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 CSSA DBS Confidentiality Agreement and received appropriate training, are approved to process applications, carry out the ID verification process and permitted access to Disclosure documentation.

All applications to the DBS must be counter-signed. Counter-signatories are approved by the CSSA Lead Signatory and cannot countersign applications until:

- their own DBS application has been approved by the DB, and they have been given a counter-signatory number;
- they have undertaken mandatory counter-signatory training with CSSA:
- they have signed the CSSA 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 CSSA eBulk 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 CSSA), 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 CSSA 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, while 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 public. Such information must be protected from inappropriate access and unauthorised disclosure. Any requests for disclosure of information relating to e-Bulk, including any made under the Freedom of Information Act should be referred to CSSA (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 or where another lawful basis or bases for processing exists.

## 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 an appointment (or other relevant) decision has been made, CSSA and its agents do not keep Disclosure information for any longer than is necessary. The retention period for all DBS related documentation is set out in the CSSA record retention schedule. If it is considered necessary to keep Disclosure information for longer than the time period set out in the record retention schedule, we will consult the DBS and consider the rights of the data subject under the General Data Protection Regulation, the Data Protection Act and the Human Rights Act 1998 before doing so. Throughout this time, the requirements set out above regarding the safe storage and strictly controlled access will continue to apply. Any retention beyond that set out in the record retention schedule will be limited to the minimum period necessary.

CSSA and its agents must not make or keep any copy or representation of the contents of a Disclosure. CSSA and its agents will, however, keep a record, on the national database, 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 appointment decision taken. The national database holds a record of all DBS applications and is checked by agents of CSSA across England and Wales, before a new DBS application is made, to ensure that applications are not made where an appropriate DBS Disclosure Certificate already exists.

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. Retention of records

The timescales for the retention of DBS related records are set out in the CSSA safeguarding record retention schedule.

<u>Safeguarding self-declaration form (SSD)</u>

The SSD will be retained by the safeguarding office that is processing the DBS application.

<u>ID verification form</u>

The ID verification form, which the applicant completes for the purposes of identity verification at interview stage and is presented at that time by the applicant along with original documentary evidence of identity, is to be retained by the appropriate countersignatory or safeguarding office that is processing the DBS application.

In the event of the application being withdrawn before completion, then the ID verification form can be destroyed by secure means as outlined in section 7 below.

ID evidence – photocopies of documents

The photocopies of original identity documentary evidence (taken originally at interview or ID verification stage are submitted by the ID verifier to the safeguarding office that is processing the application and are retained by that office until the Disclosure process has been completed. If there are questions about accuracy of content of the DBS Disclosure, then the ID documents should be retained until the matter is resolved and then disposed of securely.

Registered Body handling of the Disclosure Certificate

Where the Registered Body or its agents need to see the original copy of the DBS Disclosure Certificate (e.g. to risk assess disclosure information), the original Disclosure Certificate must be returned to the applicant by secure post e.g. signed for or tracked, once the risk assessment process has concluded.

## 7. Disposal

Once the retention period has elapsed, CSSA and its agents will 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 will 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.

## 8. 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,) CSSA 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.