



Bringing people closer to Jesus Christ through His Church

## **Catholic Diocese of Portsmouth**

Registered Charity no. 1199568

# Policy DBS processing.

**Version 1 – July 2021**  
**For review – July 2023**



## **DBS Processing**

As a Regulated Affiliate of the Catholic Safeguarding Standards Agency (CSSA), the Diocese adheres to the national policies and practice guidance as defined by the 'One Church' approach.

Our safeguarding services and functions are administered in accordance with the agreed national safeguarding standards which provide the framework for safeguarding activities across the Catholic Church in England and Wales.

The Catholic Safeguarding Standards Agency (CSSA) is registered with the DBS on behalf of the Catholic Church in England and Wales.

The DBS Disclosure application and assessment process is implemented on behalf of the CSSA, via authorised agents in dioceses, eparchies, religious congregations and Catholic organisations. Signed agreements exist with these agents whereby they agree to abide by the policies and procedures of CSSA and the DBS.

The Registered Body (CSSA) is not responsible for undertaking DBS Disclosures where these are already carried out via statutory organisations (for example staff in Catholic schools or staff in Catholic social welfare agencies).

The CSSA and its agents are required to abide by the DBS Code of Practice for recipients of criminal record information to ensure that any information received by the Registered Body and its agents is handled fairly and used properly.

### **[DBS Code of Practice](#)**

A breach of the DBS Code of Practice can result in the suspension or cancellation of registration.

CSSA is committed to the fair and sensitive use of disclosure information and will take all reasonable steps to ensure that it, and its agents, seek to achieve and maintain the highest standards of practice. CSSA has an [Information Security Policy](#).

Where an applicant feels that disclosure information has not been handled in a fair and sensitive way an appeal process is available using the [policy for handling DBS related complaints](#).

Failure to comply with requirements set out in the prevailing Data Protection legislation may also result in enforcement action from the Information Commissioner's Office.

## Types of DBS Disclosure

Different roles are eligible for different types of criminal record checks. Eligibility is determined by the nature of the activity undertaken by the person.

### Basic check

The basic check can be used for any position or purpose. A basic certificate will contain details of convictions and cautions from the Police National Computer (PNC) that are considered to be unspent under the terms of the Rehabilitation of Offenders Act (ROA) 1974.

### Standard check

The standard check is available for duties, positions and licences included in the Rehabilitation of Offenders Act (ROA) 1974 (Exceptions) Order 1975, for example, court officers, employment within a prison, and Security Industry Authority (SIA) licences.

A standard level certificate contains details of all spent and unspent convictions, cautions, reprimands and final warnings from the Police National Computer (PNC) which have not been [filtered in line with legislation](#).

### Enhanced check

The enhanced check is available for specific duties, positions and licences included in both the Rehabilitation of Offenders Act 1974 (Exceptions Order 1975) and the Police Act 1997 (Criminal Records) regulations, for example, regularly caring for, training, supervising or being solely in charge of children, specified activities with adults in receipt of health care or social care services and applicants for gaming and lottery licences.

An enhanced level certificate contains the same PNC information as the standard level certificate but also includes a check of information held by police forces.

### Enhanced with Barred List check(s)

The enhanced check with barred list check(s) is only available for those individuals who are carrying out regulated activity and a small number of positions listed in Police Act 1997 (Criminal Records) regulations, for example, prospective adoptive parents and taxi and Private Hire Vehicle (PHV) licences.

An enhanced level certificate with barred list check(s) contains the same PNC information and check of information held by police forces as an enhanced level check but in addition will check against the [children's and/or adult's barred lists](#).

If the application includes a request to check the barred list(s) the DBS has a statutory duty to consider any information that suggests the applicant may pose a risk of harm. The DBS will write to the applicant if they are affected.

### DBS adult first check

DBS adult first is a service available to organisations who can request a check of the DBS adults' barred list. Depending on the result, a person can be permitted to start work, under supervision, with vulnerable adults before a DBS certificate has been obtained.

[More guidance regarding adult first checks can be found on the Disclosure and Barring Service website](#)

The requests carry strict criteria:

- the position must require a criminal record check by law.
- the position must be eligible for access to the DBS adults' barred list.
- the organisation must have requested a check of the DBS adults' barred list on the DBS application form.

The DBS' reply to an adult first check request will contain one of the following responses and will clearly state that it only forms the first part of the criminal record check application process and that further information will follow:

- option 1: 'Registered Body must wait for the DBS certificate'.
- option 2: 'no match exists for this person on the current adults' barred list'.

If the adult first check indicates that the Registered Body must wait for the DBS certificate, the details provided may have indicated a match on the DBS adults' barred list. However, further investigation is required to confirm this and you should await the certificate. Alternatively, the check will state that no match exists for the individual on the adults' barred list.

The DBS charge for the Disclosure service per application. Current fees can be found on the DBS website. However Disclosures are free of charge for volunteers that meet the DBS definition.

## Eligibility for DBS Disclosure applications.

A DBS check cannot be undertaken on anybody below the age of 16 years. The appointment of a person under the age of 18 years to a role that is eligible for a DBS check requires careful consideration of their capability, experience and training to ensure that they can fulfil the responsibilities of the role. It is highly recommended that young people under the age of 18 years are not engaged in regulated activity within the Catholic Church in England and Wales.

**Before asking somebody to apply for a DBS check you are legally responsible for making sure that the job role is eligible. This should be done before a counter-signatory signs an application.**

The guides below will help you identify the type of workforce that an applicant will be working in and the level of check that the role is eligible for.

### Adult workforce guide

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/735504/Adult\\_workforce\\_guide\\_v10\\_0\\_030818.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/735504/Adult_workforce_guide_v10_0_030818.pdf)

### Child workforce guide

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/804668/Child\\_workforce\\_guide\\_v10\\_0\\_28052019.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804668/Child_workforce_guide_v10_0_28052019.pdf)

The DBS has an online eligibility tool which provides useful assistance. The tool is not intended to act as legal advice and does not cover every role.

### [DBS Eligibility check tool](#)

### Regulated activity.

Regulated activity is work that a barred person must not do. Regulated activity excludes family arrangements and personal, non-commercial arrangements.

Guidance about [regulated activity with children](#) has been published by the Department for Education (DfE).

Information about [regulated activity with adults](#) is available from the Department of Health (DH).

### Supervision of children.

Statutory guidance on supervising activity with children, which is regulated activity when unsupervised can be found here [Supervision of activity with children](#)

### Role list.

The 'role list' sets out the default levels of Disclosure that particular roles within the Catholic Church in England and Wales are eligible for.

Decisions about eligibility for different levels of Disclosure are based on the description of the activities undertaken by the particular role.

The roles listed within Ebulk have default levels of Disclosure set against them. These are periodically reviewed and updated when changes are made to the role list. All requests for additions or alterations to the role list should be made to the CEO of the CSSA. If changes are made to the role list, the corresponding changes will be reflected in Ebulk.

Although defaults are set, roles are not always definitive and sometimes it will be necessary to override the default setting to take account of variations within a particular role. For example, where the default is set to 'enhanced disclosure' only but the expectation of the role is that it will include regulated activity, the correct level of Disclosure to be applied for should be overridden with an 'enhanced disclosure with barred list check'.

### Overseas criminal record checks.

The DBS cannot access criminal records held overseas and a DBS check may not provide complete view of an applicant's criminal record if they have lived outside of the UK. Employers should make sure that they have access to all the information available to them to make a safer recruitment decision. Overseas criminal record checks can be obtained by the Registered Body Ebulk provider First Advantage.

### Seminarians and Religious in Formation.

Disclosures for Seminarians and Religious in Formation will be undertaken according to the national selection procedures for acceptance to being in priestly or religious formation.

The Vocations Director or equivalent in the Diocese or Religious Congregation of origin will:

- Initiate the Disclosure application.
- Verify identity before sending the Disclosure application to the counter-signatory for signature.
- Ensure that the Safeguarding Self Declaration form and Identity Verification forms have been completed and ensure details of the applicant are added onto the National Database.

The Vocations Director must check that the application form has been completed accurately to ensure the DBS process is not delayed due to omissions on the form.

CSSA recommends that applications for Disclosures are submitted at least 2 months prior to the departure of the applicant in an attempt to obtain the required clearance prior to the student arriving at the seminary or religious formation house.

It is not necessary for a Disclosure to be undertaken when a transfer of institution for a seminary student takes place as the documentation should travel with the student.

When the Disclosure process is completed, the counter-signatory will inform the Vocations Director or equivalent, which will in turn ensure that the appropriate Rector/Congregational Leader, or equivalent, is informed of the outcome.

The counter-signatory is responsible for ensuring that Vocational Directors and Rectors (and equivalents) are aware of and abide by the CSSA Safer Recruitment policies and DBS Codes of Practice.

#### Application forms for DBS Disclosures.

Once eligibility has been determined, the application can be made to the DBS. If an application is not being made via e-bulk, there is full guidance (for applicants; ID verifiers and countersignatories) on how to complete a paper application form available from the [DBS website](#).

#### Role Titles to be used when submitting an application for a Disclosure:

- **X61 line 1:** You must include the relevant workforce(s). Choose the appropriate:
  - Child Workforce;
  - Adult Workforce;
  - Child and Adult Workforce.
- **X61 line 2:** Enter a description of the 'position applied for' up to 30 characters.

*Please note that the Workforce must be stated on the Disclosure Application to enable the individual to make use of the Online Update Service. Failure to include the relevant workforce on the first line of X61 will lead to delays in the application being processed as the Police Disclosure Units will query which workforce the role will be working with and prohibit the individual from using the Disclosure for similar roles with other organisations.*

#### Some illustrations:

- Children's Liturgy - Line X61 should show CHILD WORKFORCE on the 1st line and CHURCH MINISTRY on the 2nd line;
- Care Staff (in a Care Home) - Line X61 should show ADULT WORKFORCE on the 1st line and CARE WORKER on the 2nd;
- For Clergy and Religious - Line X61 should show CHILD AND ADULT WORKFORCE on the 1st line and either PRIEST or RELIGIOUS BROTHER/SISTER on the 2nd.

### Guidance on role titles:

Role titles on the DBS application form must indicate the nature of the role and the contact involved so the eligibility of the Disclosure is apparent for DBS processing purposes.

Therefore, for post-holders (for volunteer roles - see below), ensure that the role indicates the nature or the element that makes it eligible for the Disclosure as opposed to the official job title which may not make the eligibility apparent to the DBS and Police Disclosure Units. The DBS can query applications that they believe do not appear to be eligible for a Disclosure to ensure that each application has been properly assessed for eligibility.

Applications in respect of Priests, Religious Sisters/Brothers etc. should be submitted using those role titles on the Disclosure Application form.

### Volunteer roles:

For all voluntary roles within the Church, the role title on the Disclosure Application Form (including Ebulk) should be entered as 'Church Ministry' or the title of the specific role as depicted on the role list. Please note that 'Volunteer' alone must not be stated on the 'Role Applied For' on the Disclosure application.

This title must be used as the nature of the work or contact will not be understood by the local Police forces when assessing church role titles such as Children's Liturgy or Eucharistic Minister etc. for relevant criminal conviction information.

\*When CSSA is operating as an Umbrella Body on behalf of Catholic organisations with their own charitable status, it is for the employing/appointing organisation to determine the role title. CSSA countersignatories can raise questions about the role on the basis of eligibility however the 'employer' determines the role title for DBS Disclosure purposes.

**Volunteer status** must only be granted in accordance with the DBS definition of a volunteer which is defined in the Police Act 1997 (criminal records) Regulations 2002 as:

"Any person engaged in an activity which involves spending time, unpaid (except for travel and other approved out of pocket expenses), doing something which aims to benefit some third party and not a close relative".

To qualify for a free-of-charge criminal record check, the applicant must not:

- Benefit directly from the position for which the DBS application is being submitted;
- Receive any payment (except for travel and other approved out-of-pocket expenses);
- Be on a work placement;
- Be on a course that requires them to do this job role;
- Be in a trainee position that will lead to a full time role/qualification.

For a copy of the DBS application process for volunteers booklet see:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/442312/DBS\\_Volunteers\\_Leaflets\\_A5\\_4pp.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/442312/DBS_Volunteers_Leaflets_A5_4pp.pdf)

**Follow this link for more information about volunteer applications**

<https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers#volunteer-applications>

As part of the application process, the applicant's identity must be verified.

#### Identity (ID) Verification.

The DBS Code of Practice <https://www.gov.uk/government/publications/dbs-code-of-practice> requires that CSSA as a Registered Body of the DBS, and its agents (countersignatories and ID verifiers) must:

- Verify the identity of the applicant prior to the submission of an application for a DBS check by following the current guidelines issued by the DBS <https://www.gov.uk/government/publications/dbs-identity-checking-guidelines>
- Ensure that any person undertaking identity verification checks on their behalf follows the current guidelines issued by the DBS;
- Make sure that lead or countersignatories do not validate their own applications for any DBS procedures.

ID Verification must be undertaken using Forms DBS [3a](#), [3b](#) or [13](#).

ID verifiers must:

- Follow the checking process as outlined in the DBS guidance <https://www.gov.uk/government/publications/dbs-identity-checking-guidelines/id-checking-guidelines-for-dbs-check-applications> using the list of Groups 1; 2a and 2b documents <https://www.gov.uk/disclosure-barring-service-check/documents-the-applicant-must-provide->
- Check and validate the information provided by the applicant on the application form / continuation sheet;
- Ensure that the application form is fully completed and the information it contains is accurate;
- Establish the true identity of the applicant through the examination of a range of documents as set out in the DBS guidance;
- in the first instance, seek documents with photographic identity (e.g. passport, photo-card driving licence, etc.) and for this to be compared against the applicant's likeness;
- Ensure all documents are in the applicant's current name;
- Ensure that the applicant provides details of all names by which they have been known and provides documentary proof to support the change of name. If the applicant is unable to provide proof to support the change of name, you should

hold a probing discussion with the applicant about the reasons why, before validating their identity;

- Ensure that the applicant provides documentary evidence of their current address, and details of all addresses where they have lived in the last five years (providing documentation where possible); cross-match the applicant's address history with any other information provided such as their CV. This can highlight if an address has not been given e.g. if the applicant's CV shows that they have worked in Liverpool in the last five years, but the application form only shows London addresses, you may wish to question the applicant further about this
- ensure one document confirms the applicant's date of birth;
- only accept valid, current and original documentation (not photocopies);
- not accept documentation printed from the internet e.g. internet bank statements;
- not accept the foreign equivalent of an identity document if that document is listed as '(UK)' on the list of valid identity documents.

A document from each of the groups should be included only once in the document count e.g. do not accept two bank statements as two of the required documents, if they are from the same bank;

Clarification must be sought from the applicant if there are any discrepancies in the information provided by the applicant and/or the identity documents supplied, and fraud is not suspected. Failure to do this may compromise the integrity of the DBS service and introduce risk into the recruitment process.

ID Verifiers must not attempt to amend the application form without the applicant's knowledge and agreement, as it will invalidate the declaration by the applicant and may breach data protection legislation.

The ID Verification Form must be completed at the same time as the ID verification is undertaken and signed off (once the documents have been checked for signs of tampering, fraud and to ensure they are in date) by the ID Verifier to confirm the documents produced are acceptable and valid.

For paper applications, and online applications via Ebulk, the original documents must be photocopied and attached to the ID Verification Form so that the counter-signatory can be satisfied that identification has been correctly verified before they countersign the application.

Also as part of the process, applicants are required to complete the DBS4 Safeguarding Self-declaration form. Criminal record disclosed on this form should be treated in the same way as information disclosed on the DBS Disclosure Certificate (see later section on blemished disclosures).

Before submitting to the DBS, the application form must be signed by a countersignatory.

### Countersignatories.

Countersignatories in dioceses, eparchies and religious congregations sign off DBS applications and are responsible for ensuring that the applicant is eligible for the check being applied for, and for ensuring the security of the sensitive personal information that they have access to.

All applicants for countersignatory status are checked by the DBS to the level of an Enhanced DBS Check. The information requested on the countersignatory application form is used to check that the applicant is suitable to see DBS certificate information.

Countersignatory applications must be proposed by the applicant's line manager and approved by the 'Lead Countersignatory' (CEO of CSSA). The applicant's line manager must submit a signed 'Countersignatory Agreement' (DBS10) to the CSSA at the time of the proposal.

On receipt of the completed and signed Countersignatory Agreement, CSSA will arrange for the DBS countersignatory application form to be sent to the applicant and for ID verification and countersignatory training.

Once the Lead Countersignatory has verified identity and checked the form, the form will be submitted to the DBS for processing. The DBS does not notify CSSA if the application is approved and fully processed. Therefore, when the newly appointed countersignatory receives their letter of confirmation (which includes a specific countersignatory reference number) a copy must be sent to CSSA without delay.

### Removal of Authorised CSSA Registered Body Countersignatories

It is a DBS Code of Practice requirement that Registered Bodies manage and maintain an accurate list of active countersignatories.

When a countersignatory resigns or no longer fulfils the countersignatory role, the office concerned must complete notify CSSA by email providing the countersignatory's name and date when the role will end.

The Lead Countersignatory of the Registered Body will write to the DBS advising of the countersignatory to be removed from the Registered Body.

### National Database

Application information is added to the national database, including whether a risk assessment is undertaken if there is a self-disclosure or DBS disclosure of criminal record or relevant information, and whether the applicant is appointed to the role they applied for.

Safeguarding roles that include DBS processing generally require access to the National Database. The Head of Safeguarding will decide who needs this access within their team.

Access to the database is approved by CSSA and before access is granted, the role holder is required to provide a completed and signed Confidentiality Agreement.

[The Agreement can be downloaded here](#) or a copy can be obtained from CSSA. The Agreement must be completed and returned before CSSA will permit access the Database.

It is each office's responsibility to notify CSSA when members of staff leave employment in order that their login credentials are made inactive to prevent unauthorised access to the National Database.

Further details concerning use of the National Database are provided within the Database User Guide.

#### 'Blemished' safeguarding self-declaration (SSD) and/or 'blemished' DBS Disclosure certificates.

Content voluntarily revealed by an individual on the safeguarding self-declaration form must be assessed in the same way as that contained within a DBS Disclosure Certificate.

#### Dioceses and religious congregations

Individuals should not be appointed to a role until the DBS Disclosure outcome is known and has been assessed for risk.

Where the information provided in the self-declaration or the DBS Disclosure outcome indicates risk to children or adults because of the person's presence or role within the parish or religious congregation, the safeguarding office that is processing the application will liaise with the appointing person, who is responsible for ensuring that the person is informed about the safeguarding measures that will be established in relation to their role, and the process that will be followed and likely timescales.

The safeguarding office will provide advice in respect of managing any perceived immediate risk and can assess future potential risk. This may include steps such as temporarily stepping the person down from an appointment pending risk assessment, referral to the statutory agencies, and making arrangements to manage risk whilst supporting continued participation in worship.

Where the DBS Certificate applicant is not already appointed and there is no current risk to children or adults within the parish or organisation, the safeguarding office and appointing person, in consultation with HR where appropriate, should consider whether it is appropriate to proceed with the Disclosure application.

#### Disclosure results

Recommendations regarding suitability to work with vulnerable groups are made at the diocesan safeguarding office level but appointment decisions are the responsibility of the appointing organisation/person.

Once a Disclosure application has been processed by the DBS, a copy of the Disclosure will be sent to the applicant directly from the DBS. For paper applications the applicant must provide the original certificate to the safeguarding office.

E-bulk applications are notified electronically to the safeguarding office when they have been completed by the DBS and the Disclosure outcome will be made available electronically to the countersignatory.

For e-bulk applications, if the electronic notification of the outcome advises that the original certificate must be seen then the applicant must submit the original certificate to the safeguarding office. Although the electronic notification via Ebulk can be relied upon e.g. 'clear', the DBS advise that paper certificates should always be seen in case of any error with what the system reports.

Where it is necessary to see the DBS Disclosure Certificate, individuals must submit their original certificate to their safeguarding office within 28 days from the date of issue stated on the certificate and be asked to confirm the accuracy of the Disclosure information. Failure to submit the Disclosure to the countersignatory within this timeframe will require that a new Disclosure application be completed because the accuracy of the former Disclosure will not be assured after 28 days.

The online DBS tracking service <https://www.gov.uk/disclosure-barring-service-check/tracking-application-getting-certificate> can be used to identify when DBS Disclosure Certificates have been returned to the applicant.

If the DBS Disclosure Certificate is 'clear' (meaning it contains NO conviction information) the safeguarding office can notify the appointing person(s) who must ensure that the individual who takes up the role is the same person who underwent the pre-appointment process.

If the DBS Disclosure Certificate is 'blemished' (meaning it contains conviction information), where there are offences that are not considered to be relevant to the role or to pose a risk in this particular appointment, the safeguarding office can advise the appointing person that there is no DBS Disclosure reason for not proceeding with the appointment.

Where there are relevant offences in relation to the person's role, the person responsible for the appointment should be notified not to proceed with the appointment until the risks have been assessed by the safeguarding office. The Disclosure should be recorded on the National Database as 'risk assessment pending'.

Where the disclosure content is similar to the self-declaration the applicant should be notified that the safeguarding measures already put in place are to be maintained until the disclosure has been further assessed and reviewed and a final appointment decision reached.

Where the disclosure certificate provides information that is different to or was not included on the self-declaration and indicates risk to children or adults because of the person's presence or role within the parish or organisation, the safeguarding office that is processing the application will liaise with the appointing person who is responsible for ensuring that the person is informed about the safeguarding measures that will be established in relation to their role, and the process that will be followed and likely timescales.

In order to risk assess the conviction information, clarification of certain issues might need to be sought from the applicant e.g. context of the offence or discrepancies between information provided on the SSD and the Disclosure Certificate. The Head of Safeguarding should arrange to meet the individual in person (or if that is not feasible arrange a discussion) within 14 days and at that face to face meeting revalidate their identity against the identification documents presented at the time the Disclosure application was verified.

If minor clarifications are required, a telephone call, letter or email exchange can replace the face to face meeting. The information discussed at the face-to-face meeting or telephone discussion should be recorded in writing and a copy submitted to the applicant for them to confirm its accuracy before recommendations are made to the appointing person.

Having clarified any discrepancies and gathered any additional, explanatory or contextual information, the Safeguarding Coordinator will review the information and assess risk. The National Database must be updated with the date of the risk assessment.

The decision to appoint volunteers generally rests with the parish priest. The role of the Head of Safeguarding is to recommend whether or not an appointment should go ahead or whether an appointment should go ahead but with certain provisions or restrictions. The appointment decision is to be recorded on the national database

The Head of Safeguarding and person with responsibility for the appointment decision will decide who is responsible for informing the person of the outcome.

If the person can be appointed, local arrangements must be made to ensure that the individual who takes up the role is the same person who underwent the pre-appointment process.

The decision in relation to clergy, religious and employees rests with the person responsible for the appointment e.g. Bishops and religious leaders for clergy and religious, and HR for employees. The Head of Safeguarding presents a written recommendation, with reasons for the recommendation, to the person with responsibility for the appointment who will take the final decision. The person with responsibility for the appointment should be apprised of the content of the Disclosure which they must handle in line with the DBS code of practice and not disclose it to anybody else.

The appointment decision is to be reported back to the Safeguarding Office who will update the National Database. The person with responsibility for the appointment decision will decide who is responsible for informing the person of the outcome.

### Umbrella Body organisations

Where the Safeguarding Self Declaration form or DBS Disclosure outcome relates to somebody within a Catholic organisation for which DBS applications are processed under an 'Umbrella Body Agreement', the Head of Safeguarding will liaise with the Safeguarding Lead within that organisation and provide advice on risk. The appointing organisation is ultimately responsible for its own risk assessment and for the decision to proceed with the recruitment process and appointment.

If there are concerns about the decision taken being contrary to the advice of the Head of Safeguarding, further recommendations should be made to the person with ultimate responsibility for the appointment decision. If concerns remain about the appointment decision the matter should be referred to the Bishop who has ultimate responsibility for agreeing who undertakes ministry in his diocese.

The Catholic Safeguarding Standards Agency (CSSA) can be contacted for advice in the event there is uncertainty about how to proceed in light of information declared on a safeguarding self-declaration form or the DBS Disclosure outcome.

Appointment decisions in relation to individuals in Catholic organisations must also be updated on the National Database.

If the person can be appointed, the person responsible for the appointment must ensure that the individual who takes up the role is the same person who underwent the pre-appointment process.

### Assessing relevancy of conviction information and risk

The Head of Safeguarding will undertake the risk assessment process only where the information contained in the Disclosure relates to the safety of children or adults. Where other information regarding convictions etc. is given on the DBS Disclosure Certificate, the Head of Safeguarding will inform the person with responsibility for the appointment within the diocese or the religious congregation who will take a decision on whether to appoint.

If it is the case that the information provided in the DBS Disclosure Certificate contradicts information provided by the applicant on the safeguarding self-declaration form, this should be explored during the meeting with the Head of Safeguarding, and the reasons why recorded in the meeting notes.

An applicant's criminal record should be assessed in relation to the tasks he or she will be required to perform and the circumstances in which the work will be carried out. This can be done using the [Blemished DBS Disclosure Risk Assessment Form](#).

### Returning the original DBS Disclosure Certificate to the applicant

The safeguarding office will return the original certificate to the applicant by 'signed for' post or alternatively where a number of applications have been submitted via the same parish or establishment (i.e. a Care Home), the certificates can be placed inside separate, addressed and sealed envelopes and sent via secure post to the Parish Representative or relevant person/recruiting person who will then pass the sealed envelopes onto each individual.

### Requests to reveal disclosure information to a third party

It is an offence to disclose information contained within a DBS certificate to any person who is not a member, officer or employee of the Registered Body or their client, unless a relevant legal exception applies<sup>1</sup>. The Head of Safeguarding should anonymise information shared with sub-committees for the purposes of decision making.

There may be circumstances where a recipient of disclosure information is asked to reveal details of a Disclosure to a third party in connection with legal proceedings i.e. in a case submitted to an Employment Tribunal. In such instances, the recipient of disclosure information should inform the Disclosure & Barring Service (DBS) of any such request immediately and prior to the release of any information.

### Renewal of criminal record checks

There is no official expiry date for criminal record check Disclosure Certificates issued by the DBS but **it is the policy of the Catholic Church in England and Wales to renew checks every 3 years for eligible roles.**

It is at the discretion of the safeguarding office to determine whether a new application for disclosure should be made or whether a status check of a Disclosure Certificate (for those individuals who have subscribed to the Online Update Service) is necessary.

Before deciding whether a new Disclosure Certificate should be applied for the following should be considered:

- The workforce relating to their last Disclosure Certificate might not be correct for the position that you are recruiting to (on an enhanced check, the police disclose information based on the workforce for which the criminal record check was originally applied for);
- The level of check for their last Disclosure Certificate may not be correct for the position you are recruiting to (e.g. a change to or from 'Regulated Activity');
- Whether the information revealed on the Disclosure Certificate was based on identity that was checked by another Registered Body.

---

<sup>1</sup> These are not defined by the DBS

If a relevant disclosure has been obtained by the CSSA Registered Body or a status check has been made using the Online Update Service, it is not necessary to apply for a new Disclosure Certificate in the following circumstances:

- Continuation of the same role previously performed but moving parish or diocese;
- Application for a role where the workforce and level of disclosure required is the same as that to which the original disclosure relates;
- Temporary deployment to a diocese of members of a religious congregation who have a Disclosure Certificate via the CSSA Registered Body.

#### Online update service.

The CSSA Registered Body supports the use of the DBS update service for the checking of Disclosure information in relation to both new appointments and existing appointments, where the role is eligible for a DBS check.

The DBS update service allows:

- Applicants to keep their DBS Disclosure Certificates up to date;
- Employers/appointers to check a DBS Disclosure Certificate.

The employer or appointer can only make the status check if they could also legally request a new DBS application for the role the individual will be working in.

#### Benefits of joining the update service

The applicant will be able to take their DBS certificate from one job or role to the next unless:

- The employer or appointing organisation asks them to apply for a new certificate;
- A certificate is needed for a different 'workforce' e.g. the existing certificate is for the child workforce and the new job or role is for the adult workforce;
- A different level certificate is needed e.g. the existing certificate is enhanced but the new job or role is regulated activity and a barred list check is required.

The applicant manages their own subscription online. The applicant can check the certificates that they have registered with the service, add or remove certificates, view those organisations that have used the service to check their certificate, update contact details and renew or cancel their subscription.

Once an individual has joined the update service, with their consent, their employer, or appointer, can go online and carry out a free of charge and instant 'status check' to find out whether the information contained on the DBS certificate is current.

#### Registering to use the update service

Applicants need to register to use the update service (see <https://www.gov.uk/government/collections/dbs-update-service-promotional-material> for further information). There is an annual fee but there is no charge for volunteers.

There is no charge for organisations to carry out an online status check.

If an applicant has not yet applied for a DBS check they can register for the update service using their application form reference number. The DBS must receive their application form within 28 days of registering for the update service. This might not be possible if there are errors or queries on the application form that require resolution before submission to the DBS. For this reason, we recommend that applicants register for the update service after their Disclosure Certificate has been issued. This must be done within 30 days of the certificate being issued.

To enable individuals to reuse their DBS certificates and the update service, the relevant workforce must be included in line 1 and the position applied for in line 2 of the original paper application and at the relevant place on e-bulk applications.

#### Gaining consent to carry out a status check

This consent is obtained when the applicant signs the declaration on the Safeguarding Self-declaration (SSD) form.

#### Withdrawing consent for the employer/appointing organisation to carry out a status check

To withdraw consent for the Church to carry out a status check, the applicant should contact the safeguarding office and arrange completion of form DBS5. Verbal instruction must be followed up with written confirmation by letter or email which can be appended to the form. This form must be filed with the original safeguarding self-declaration (SSD) form which provided the initial signed consent.

#### Before carrying out an online 'status check'

For safeguarding personnel, counter-signatories and employers:

Before carrying out a status check you will be asked to complete a legal declaration confirming that you have the permission of the individual and that you have the legal right to ask the exempted question; that is the legal right to request for a person to reveal their full criminal history, including spent convictions but excluding protected cautions and convictions that will be [filtered from a criminal record check](#). By making this declaration you are saying that you have the right to be given the information to make a suitability assessment and the information is at the level you are legally entitled to request in relation to the role you are recruiting for.

The following must be fulfilled before you carry out a status check.

- The role must be confirmed as being eligible for a DBS check;
- The DBS Certificate must contain the exact workforce that you are entitled to know about for the role you are recruiting/appointing to e.g. If the applicant's existing Certificate is for the adult and child work force and they are now applying for a role with/or working within the child workforce only, the applicant would be required to apply for a new check;
- The applicant must be legally entitled to the same level of DBS Certificate e.g. enhanced or enhanced with barred list e.g. If their existing check is enhanced with an adult barred list check and they are now applying for a role which only

requires an enhanced check, or a check of the child barred list, the applicant would be required to apply for a new check;

- The applicant must have given their permission for the check;
- The original Disclosure Certificate must have been seen by the person carrying out the status check (it is not sufficient to be sent a photocopy or scanned image of the certificate based on current DBS guidance);
- The identity of the individual must be verified and checked against the information held on the original Disclosure Certificate (same name and date of birth).

Applicants must always be asked if there has been a name change since their last disclosure certificate and if there has been, they must apply for a new check regardless of whether the original check was carried out by CSSA or another Registered Body. They are then able to link the two checks together on their update service account for the purposes of future update checks.

#### Consent to undertake a status check

##### DBS Certificate originating from another Registered Body

Consent to undertake the check will be obtained via the safeguarding self-declaration (SSD) form. In all cases, the original Disclosure Certificate must be seen and the person's identity verified as if a new check were being undertaken by the CSSA Registered Body.

##### DBS Certificate originating from the CSSA Registered Body

Although the applicant will have given consent on the original SSD for the CSSA Registered Body to undertake periodic status checks, before the status check is carried out, the applicant must be asked to declare any changes to their circumstances e.g. a change in workforce or type of activity, a name or address change. If there is a change in name, a new disclosure will need to be applied for.

The applicant should be offered the opportunity to complete a new SSD which they can send to the safeguarding office, to declare any relevant changes in criminal record

#### Identity verification for a status check

##### DBS Certificates processed by the CSSA Registered Body via the same diocese, congregation or organisation

It is not necessary to request sight of the original DBS Certificate or undertake new identity verification if there are clear records to demonstrate that the original certificate, or outcome on Ebulk, was seen and identification was verified when the original disclosure was undertaken.

For example, there is an entry on the national database and the original ID verification form can be checked. If for any reason the person carrying out the status check is not satisfied that they can verify the identity of the individual using existing records, they should undertake identity verification in line with the processes below.

### DBS Certificates processed by the CSSA Registered Body but via a different diocese, congregation or organisation

For applicants whose check was originally carried out and recorded by the CSSA Registered Body but via a different diocese, religious congregation or organisation, the original certificate must be seen and identity verified before a status check is carried out. The 'update service identity verification' form (DBS13), can be used for this purpose if full identify verification has already taken place when the person was appointed to the role. If the applicant's identity has not already been verified as part of the appointment process, then the process for applicants whose DBS Certificate was processed by a different Registered Body must be followed.

For applicants whose original check was carried out by the CSSA Registered Body but are required to re-verify their identity it is advised that as a minimum, the applicant provide one of the eight documents listed on the [update service identity verification form \(DBS13\)](#) which have been taken from groups 1 and 2a of the DBS ID verification guidelines. It is the responsibility of the person carrying out the status check to establish the identity of the applicant and this is the minimum standard recommended. If the person carrying out the status check is unable to satisfy themselves as to the identity of the individual then a new check should be requested.

If the person undertaking the ID verification is not the same person carrying out the status check, photocopies of the identification documents and the DBS status check identity verification form (DBS13) must be provided to the person carrying out the status check.

All documentation should be kept in accordance with the record retention policy.

### Undertaking an online status check

Go to [Gov.uk](https://www.gov.uk) and search for "DBS Update Service".

The online system will require that the following information is entered by the person undertaking the online status check:

- The name of the organisation;
- The forename and surname of the person conducting the online check;
- The details of the DBS certificate being checked;
- The DBS certificate number;
- The current surname of the DBS certificate holder as shown on their DBS certificate;
- The date of birth of the DBS certificate holder in the format DD/MM/YYYY, as shown on the DBS certificate.

The system will present a legal declaration which should be read before ticking the "I agree with the legal declaration" check box to proceed.

A result for the entered information will be presented on screen. The person undertaking the online status check must print a copy of the result as evidence of the check being undertaken and return this to the applicant with their original Disclosure Certificate. The result must be entered onto the national database and

handled in the same confidential manner as content on the Disclosure Certificate itself.

The result will provide one of the following statements:

1. This DBS certificate did not reveal any information and remains current as no further information has been identified since its issue. This means:
  - The DBS certificate when issued was blank (it did not reveal any information about the person);
  - No new information has been found since its issue and can therefore be accepted as still being current and valid.
2. The DBS certificate remains current as no further information has been identified since its issue. This means:
  - The DBS certificate revealed information about the person;
  - No new information has been found since its issue and can therefore be accepted as being still current and valid.
3. The DBS certificate is no longer current. Please apply for a new DBS check to get the most up-to-date information. This means:
  - New information has come to light since the DBS certificate was issued and you will need to apply for a new DBS check to see this new information.
4. The details entered do not match those held on our system. Please check and try again. This means either:
  - The individual has not subscribed to the update service;
  - The DBS certificate has been removed from the update service;
  - You have not entered the correct information.

#### Changes to Certificate status

For all DBS certificates the status will change if:

- New convictions, cautions, reprimands or warnings have been added to police records;
- An amendment has been made by the police to current convictions, cautions, warnings or reprimands.

For enhanced DBS certificates the status will change if:

- As above plus if the person becomes added to either/both barred lists.

If the status check reveals there has been a change, a discussion must take place with the individual concerned and the change must be risk assessed in line with the procedure for dealing with blemished Disclosures.

In circumstances where an individual is subscribed to the update service and the status check indicated a change to the Disclosure Certificate content which resulted in a new Disclosure application being made, the Registered Body can obtain a copy

of the resulting Disclosure Certificate from the DBS if the following conditions are met in full:

- The DBS released the new certificate to the applicant more than 28 days ago, **and**
- The applicant has not submitted their certificate to the safeguarding office.

#### Frequency of DBS searches for new information

- When a person adds their DBS certificate to their update service account, the DBS will search regularly to see if any new information has come to light since it was issued. The frequency varies depending on the level and type of DBS certificate.
- For criminal conviction and barring information the DBS will search for updates on a weekly basis.
- For non-conviction information, the DBS will search for updates every 9 months.
- The DBS will not inform the Registered Body if a status changes.

#### Duty to Refer to the DBS.

There is a legal requirement for an employer or organisation to make an online referral to the Disclosure and Barring Service (DBS) when it believes a person has caused harm or poses a future risk of harm to vulnerable groups, including children.

The following groups have the duty and the power under the Safeguarding Vulnerable Groups Act 2006 to make a referral to the DBS:

#### Duty to Refer

- Regulated activity suppliers (employers and volunteer managers); and
- Personnel suppliers.

#### Power to Refer

- Local authorities (safeguarding role);
- Education and library boards;
- Health and social care (HSC) trusts (NI);
- Keepers of registers e.g. General Medical Council, Nursing and Midwifery Council;
- Supervisory authorities e.g. Care Quality Commission, Ofsted; and
- If the person being referred to the DBS is a teacher in England they should also be referred to the National College for Teaching and Leadership.

The DBS has expert caseworkers who process referrals about individuals who have harmed or pose a risk of harm to children and/or vulnerable groups.

They make decisions about who should be placed on the child barred list and/or adults' barred list and are prevented by law from working with children or vulnerable groups.

An employer or volunteer manager is breaking the law if they knowingly employ someone in a regulated activity with a group from which they are barred from working.

A barred person is breaking the law if they seek, offer or engage in regulated activity with a group from which they are barred from working.

If the person you are referring to the DBS is a teacher in England and the allegation is substantiated and the person is dismissed or the employer ceases to use the person's services, or the person resigns or otherwise ceases to provide his or her services, the local authority Designated Officer within the local authority should discuss with the case manager and their personnel adviser whether a referral to the DBS for consideration of inclusion on the barred lists is required; and in the case of a member of teaching staff whether to refer the matter to the National College for Teaching and Leadership (NCTL) to consider prohibiting the individual from teaching (see Keeping Children Safe in Education (2015)).

Guidance on making a referral to the DBS can be found using the following link: <https://www.gov.uk/guidance/making-barring-referrals-to-the-dbs>

## **Annex 1**

### **Useful links – DBS**

#### **Useful and Related Documents/Guidance**

[Protection of Freedoms Act 2012](#)

[Safeguarding Vulnerable Groups Act 2006](#)

[Disclosure and Barring Service - GOV.UK](#)

[Regulated Activity \(Adults\) and Factual Note - Department of Health](#)

[Regulated Activity with children – Department for Education](#)

## Annex 2

### Blemished DBS Disclosure Risk Assessment Form

The assessment is designed to support the Safeguarding Office in making an informed and balanced decision about whether to appoint or allow continuation in a role where information contained on the SSD or DBS Disclosure Certificate relates to issues regarding the safety and wellbeing of adults and children in a church setting. Before any decision is reached the individual will be offered the opportunity to discuss the contents of the disclosure with the Safeguarding Co-ordinator. Offences unrelated to the safety and wellbeing of adults and children may be notified to an appropriate person in the diocese or religious congregation who has responsibility to assess their relevance to another appointment.

Name of Individual:				DOB:	
Status of individual:	An existing appointee		A new applicant		
Post applied for or already appointed to:					
Initial assessor (prior to presentation at panel):					
	Signed		Date		
What triggered this risk assessment?	<ul style="list-style-type: none"> <li>• Offences/allegations disclosed on SSD</li> <li>• Positive DBS check during recruitment</li> <li>• Disclosed during existing appointment</li> <li>• Repeat DBS check on existing appointment with new information</li> </ul>				
Discussed at panel – include names of panel members and date of decision/recommendation:					
Decision or recommendation of panel (please tick as applicable):	Appoint		Do not appoint		
* Appoint with adjustments	*Appoint with adjustments to role (give details e.g. supervision, monitoring arrangements etc.)				

Discussed with  individual – include name of person undertaking the discussion and date:	
--	--

Details of offences or other disclosed relevant information including allegations		
Offence	Date of caution / conviction	Brief circumstances behind the offence/allegation (for instance, for possession of drug offence what was applicant doing to bring themselves to the attention of police)
Do the DBS Listings (formerly POCA, POVA, and List 99) bar the appointment?	Yes/No	If the answer is yes, then the appointment is automatically unlawful and the person must not be appointed to the post. Do not continue with this decision sheet and if appropriate, contact the Designated Officer in the Local Authority.

Role description (attach where possible)
Consider who the applicant will be working with and whether the role involves responsibility for finance, items of value or other high-risk areas. This is particularly relevant where offences relate to fraud, burglary, robbery for example.

Assessment of risks regarding the person and the offence or other disclosed relevant information including allegations
Provide information about the following:

Whether the individual agrees with the information on the disclosure? Note any discrepancies or non-agreement.	
Whether the person fully disclosed the offence on the self-declaration documentation or whether the information has come to light retrospectively. What reason was given for non-disclosure and how might this affect the appointment decision?	
Whether the offence involved a child and/or an adult at risk or an adult who was vulnerable.	
The seriousness of the offence and its relevance to the safety of parishioners/service users, other employees/volunteers/church roles, or the public. Consider whether the offence had a major (significant) impact on an individual e.g. long-term, a moderate impact e.g. noticeable and medium term or minor impact e.g. limited and/or short-term impact.	
Whether the relevant offence was committed at work (either paid or unpaid work).	
Whether the role allows the opportunity to re-offend or repeat behaviours of concern.	
Whether the behaviour could pose a risk to parishioners/service users, other employees/volunteers/church roles, or the public.	
The age at which the offences were committed. Was the offence committed as an adult, young person or child? Offences that took place years ago may have less relevant now with the exception of serious violent or sexual offences for example.	
The length of time since the offence.	

Whether the offence was isolated or part of a history of offending. Repeated offences may indicate that the individual has not been able to change their offending behaviour and this may indicate likelihood of reoffending.	
Any relevant information offered by the person regarding the circumstances which led to the offence being committed. Note whether this has been corroborated and if so, by whom.	
The degree of remorse, or otherwise, and their motivation to change.	
Whether the person's circumstances have changed since the offence was committed, making reoffending less likely.	
Whether any regulatory or registration body took any action following the conviction.	
Any relevant information regarding the country in which the offence was committed e.g. some activities are offences in Scotland and not in England and/or Wales and vice versa.	
Whether the offence has since been decriminalised by Parliament.	
Are there any assessments and reports from those agencies involved in the applicant's process of rehabilitation e.g. probation service, specialists working in prison, other agencies?	

What safeguards can be put in place to mitigate identified risks e.g. level of supervision, changes in responsibilities?

--

Other relevant information.
-----------------------------

E.g. what arrangements will be put in place to ensure that there is not a change in role without further risk assessment.
---

Analysis of initial assessor
------------------------------

--

Recommendations and rationale
-------------------------------

--

Analysis and advice given to organisation with Umbrella Body Agreement
--

--

--

Form completed by and date

To be retained for 10 years and 1 day after the person leaves role.