

Update Service & New Process Guidance

The Update Service provides subscribers with a portable product that will not become 'out of date' as soon as it is issued and can be used when applying for further employment within the same workforce (children/adults). The Update Service will provide subscribers and employers with the ability go online and see whether or not their Disclosure certificate remains valid (no new information has come to light since it was issued) or whether the status has changed and a new application is needed in order to receive new information.

Two Application types

There are two types of Enhanced: Enhanced Disclosure with Barring List (EDBL) Check (where the Registered Body is eligible to request a check of the Barred Lists) and an Enhanced Disclosure (ED) Check (where the Registered Body is not eligible to request a check of the Barred Lists).

The two are differentiated quite easily: if no Barring List boxes are checked (the '*Regular Contact with Children or Regular Contact with Adults*' boxes, found within the Post Information section of the LPF search screen) the Registered Body is not eligible to ask for the applicant to be checked against the DBS Barred Lists - this is an ED Check. If one or both boxes *are* checked, the application is an EDBL Check.

Police will process EDBL Checks and ED Checks in the same way – no difference.

'Post Applied For' field

The 'Post Applied For' field on the notification screen will also capture the workforce applied for.

Two Notification types – how do they differ?

With the introduction of the Update Service, you will begin to receive two notification types: **Application Notifications** and **Pseudo Application Notifications**.

Physically, there is very little difference between the two and you process them in the same way. You can receive a Pseudo for an EDBL or an ED Check.

A Disclosure Application Notification is the equivalent of the notifications that you have been receiving since CRB commenced operations in 2002 in that they result in the issue of a physical Disclosure Certificate (EDBL or ED).

Any applicant can choose to subscribe to the Update Service after their Disclosure is issued (following the processing of an Application Notification). Once subscribed, any new information relating to an individual who is a close match with the subscriber's nominal details will generate an Update Service **Pseudo** Application Notification to forces. These notifications are known as 'Pseudo' because they are not in themselves an Application – they do not result in the issue of a physical disclosure certificate. They can be distinguished from Disclosure Application Notifications by the letter 'P' which prefixes the Application Reference Number.

An Update Service subscriber and (and their employer) will be able to check the currency of their disclosure certificate via an online check of the subscriber's Update

Service Profile Status – the profile holds all of their applications and shows the status of each of them ('current'/'out of date', as new info is available requiring a new application). If information comes to light which, in your opinion, ought to be disclosed, or if the subscriber's PNC record changes substantially, their online status will change and the applicant will need to make a new application in order to get an up-to-date certificate.

Important points to remember for Pseudo Application Notifications

A Pseudo Application Notification follows on from an Update Service subscriber's Disclosure Application Notification – Pseudos are not generated for non-subscribers. A Pseudo is generated when possible new information is identified, after the initial Disclosure has been completed and the certificate has been issued.

Pseudo notifications do not result in the issue of a certificate. However, if, after information has been assessed as normal, your decision can result in a change to the subscriber's online Profile Status, effectively making their existing certificate unusable. Should the applicant then apply again, in order to receive an up-to-date certificate, a new Disclosure Application Notification will be sent to forces, and the cycle begins again.

A Pseudo Notification is generated when **information** is detected that matches the details of a subscriber to the Update Service (the subscriber having already received a completed disclosure some time previously). Your searching for, and assessment of, new information will determine whether or not you need to disclose information.

You will only consider new information, that which has come to light since the subscriber's previous certificate was issued. You may disclose this new information or use it to re-assess information that was considered previously, but not disclosed. For example if you had discarded information at Box 4 previously but the new information leads you to believe that the information considered and discarded previously is now more likely to be true, then you can consider disclosure of both pieces of information as neither were disclosed on the original certificate.

For a Pseudo Notification, you should only disclose (enter Approved info onto CRM) when you have **new information** that you did not disclose on the previous Disclosure Application notification. Should you find that you **do not** have any new information that needs bringing to the attention of the employer **you do not enter the same disclosure text onto CRM again**. If you did this, the applicant's Update Service Profile Status would be changed automatically to 'New Application Required' and the applicant will be directed to apply for a new certificate, needlessly and incorrectly.

With a Pseudo Notification, if you believe that you need to remove some of the information that you disclosed previously, due to new information directly impacting on your previous decision, **you can only do so by raising a Dispute** – this will result in the creation of a new Disclosure Application Notification.

If you had nothing to disclose when you processed the earlier Application Notification (or if you never received the earlier Application Notification) you will disclose everything that passes QAF (dependent on whether it is an EDBL or ED).

The DBS Barring Arm

One significant aspect of the Protection of Freedoms Act is the new ability, within the Update Service, for the sharing of information between the DBS Disclosure Arm and the DBS Barring Arm.

The DBS Barring Arm is entitled to consider all applicants for inclusion in either or both of the DBS Barred Lists (Children's List; Adults List).

Information obtained by one part of the DBS business (Disclosure or Barring) may be shared with the other. All information provided by police, for an EDBL Check, as part of the Disclosure service (i.e. information that will appear on the face of an EDBL certificate) will be shared with the Barring Arm – this will be done automatically, by the DBS IT system. The Barring Arm will receive the full list of PNC offences (they will even receive those which the 'old & minor' filtering rules have removed) - **this does not apply to ED Checks.**

Relevance

For EDBL and ED Checks, relevance considerations will be led by what is recorded in the Post Applied For field on the application form. This field should record the Workforce and the Post Applied For

- Child Workforce – information relevant to any role working with children
- Adult Workforce - information relevant to any role working with adults
- Child & Adult Workforce - information relevant to any role working with either the child or the adult workforce
- Other Workforce* - information relevant to the **Post Applied For** only

*Other Workforce – posts such as those relating to gaming licensing.

The Disclosure process does not infringe upon your ability to refer ANY information to Barring that you deem to be relevant and of interest to Barring. Such referral, whilst made outside of the DBS application and Update Service process, should be made using the dedicated email address: dbsdipolice@dbs.gsi.gov.uk

ED Checks

ED Checks do not require a check against the DBS Barred.

EDBL Checks

EDBL Checks require a check against the DBS Barring Lists.