Registered Body

Disclosure and Barring Service (DBS) System

This Agreement is made between:

1. the provider of this Disclosures criminal record service and the body registered with the Disclosure and Barring Service (DBS) to countersign criminal record disclosure applications submitted via the System ("the Registered Body");

2. the customer of the Registered Body for whom the Registered Body provides a criminal record checking service via the System ("the Organisation") (if any); and

3. you, a nominated user of the System ("Authorised User").

Background

A. The Organisation operates an online service, known as Disclosures, to process and manage criminal record checks electronically. These criminal record checks will be submitted via an e-bulk channel to the DBS, allowing batches of applications to be countersigned and submitted to the DBS.

B. The Disclosures system ("the System") is provided to the Organisation by the Registered Body pursuant to the terms of a licence agreement.

In order for Authorised Users to access the System to submit and/or manage DBS applications they must agree to be bound by the provisions of this User Agreement.

Terms and conditions

1. The Organisation, and the Authorised User shall adhere to the DBS Code of Practice, The Police Act 1997 (as amended), all relevant data protection legislation, including the Data Protection Act, the General Data Protection Regulation (GDPR) and all relevant statutory provisions and guidance relating to DBS checks.

2. The Authorised User will receive appropriate training – relevant to their role in the disclosure process - from the Organisation and will be supplied by the Registered Body with secure login details to access the System. The Authorised User will be responsible for protecting their own login and password against unauthorised use. These credentials shall not be disclosed to any other person. The Authorised User is required to inform an appropriate person within the Organisation immediately if they suspect their login or password has been compromised in any way.

3. The Authorised User may be required to check an applicant's identity. This shall be carried out in accordance with the DBS Code of Practice and the identity checking guidelines published from time to time. The Authorised User shall then complete the relevant section of the electronic disclosure application form in the System.

4. The Authorised User will then grant access to the System to the applicant, who shall then complete their section of the electronic disclosure application form. The Authorised User must not complete this part of the application form on behalf of the applicant, unless specific permission has been given by the applicant to do so. Where the applicant cannot complete their own form, further guidance should be sought from the Organisation's DBS team, or the DBS.

5. Access to the System shall only be granted to those individuals entitled to request a DBS disclosure in connection with their role and those applicants for whom the Organisation is entitled to request a DBS disclosure.

6. Other than applicants whose role and relationship with the Organisation dictates that a DBS check is required, DBS checks shall not be submitted on behalf of third party organisations or individuals under any circumstances.

7. Each party to this User Agreement undertakes that it will treat as confidential any personal information obtained in relation to use of the Service. Such personal information shall be handled, used and retained in accordance with the Registered Body's policy on the handling of disclosure information. In particular, the receiving party will not disclose such personal information in whole or in part at any time to any third party, nor use the personal information for any purpose other than is necessary for the DBS application. The obligations set out in this clause shall not apply to any personal information which is required to be disclosed by statute or court order.

Breaches of terms and conditions

1. If the Authorised User is suspected of breaching the terms of this User Agreement, their access to the System may be removed temporarily by the Organisation or the Registered Body until the circumstances of the breach are fully investigated. If the Authorised User is found to be in breach of the Agreement or their obligations of confidentiality in respect of the System or the disclosure service, their access may be permanently removed or restricted.

2. Where there are serious or persistent breaches of this Agreement, the Organisation may have its access to the System removed either temporarily or permanently as deemed appropriate by the Registered Body.

3. If any breach is deemed by the Organisation or the Registered Body to be a potential criminal offence, or breach of data protection legislation, this may be reported to the Police, the DBS or other relevant authority.

4. Any costs incurred by the Registered Body as a direct or indirect result of unlawful, unauthorised or inaccurate applications (caused by deliberate actions or omissions on the part of the Authorised User) may be charged to the Organisation.