Disclosure and Barring Service (DBS) Code of Practice

1. Introduction

This document provides an overview of the Code of Practice for Disclosure and Barring Service Registered Persons and applies to all Registered Bodies with the Disclosure Service (DBS) under section 120 of the Police Act 1997 ((Registered Bodies) and recipients of Update Service information under section 116A of the Police Act 1997. The Code refers to any information exchanged between DBS and the Registered Body.

The Code of Practice applies to all recipients of disclosure Information (except where otherwise indicated). This includes:

- Registered persons
- Those countersigning disclosure applications on behalf of registered persons
- Others receiving such information

Although certificates are provided directly to the applicant, registered bodies will receive personal information related to applications and, where registered bodies are also employers, voluntary sector organisations or licensing authorities, will receive disclosure information when certificates are provided by them to their employees or applicants for posts, including volunteers.

2. Purpose of the Code

The Code of Practice is intended to ensure that the information released will be used fairly.

The Code also seeks to ensure that sensitive personal information is handled and stored appropriately and is kept only for as long as is necessary.

3. Obligations of the Code

Registration details

Registered bodies must:

- Provide up-to-date information to the DBS in respect of their registration information and counter signatories in line with current procedures.
- Maintain all accounts, online or otherwise, for all DBS products and delete when no longer required.
- Ensure any electronic system used complies with specifications set out in The Police Act 1997 (Criminal Records) (Registration) Regulations 2006.

Application process

Registered bodies must:

- Submit applications for a DBS product in the format determined by DBS.
- Ensure that applications for a DBS product are completed accurately and that all data fields determined mandatory are completed in full.
- Ensure that any application submitted electronically complies with DBS specifications as stipulated in line with current requirements.
- Ensure that, where evidence checkers complete any part of the administration of the application process, sufficient training has been provided to enable some degree of accuracy required by the DBS of the counter signatory.

Identity verification

Registered bodies must:

- Verify the identity of the applicant prior to the submission of an application for a DBS product by following the current guidelines issued by the DBS.
- Ensure that any person undertaking identity verification checks on their behalf follows the current guidelines issued by DBS.
- Make sure the lead or counter signatories do not validate their own applications for any DBS products.

Payment of fees

Registered bodies must:

- Pay all registration fees in line with time periods set out in current procedures.
- Pay all fees relating to DBS products in line with time periods set out in current procedures.
- Pay all fees related to criminal records check applications submitted after any decision by the DBS to suspend registration or deregister the organisation.
- Correctly apply The Police Act definition of a volunteer to each criminal records check application, to assert eligibility that no fee should be charged for that application.
- Publish all fees, in relevant documentation, associated with the processing of criminal records check applications when you do so on behalf of others.

Eligibility

Eligibility for DBS checks is set out in the following legislation:

Standard checks – to be eligible for a standard level DBS certificate, the position must be included in the Rehabilitation of Offenders Act (ROA) 1974 (Exceptions) Order 1975.
Enhanced checks – to be eligible for an enhanced level DBS certificate, the position must be included in both the ROA Exceptions Order and in The Police Act 1997 (Criminal Records) Regulations.
Enhanced checks with children's and/or adults' barred list check – to be eligible to request a check of the barred lists, the position must be eligible for an enhanced level DBS certificate and be specifically listed in The Police Act 1997 (Criminal records) Regulations as being eligible to check the appropriate barred list(s).

Employers commitment to disclosure information

- Ensure that all applicants for relevant positions or employment are notified in advance of the requirement for a disclosure.

- Notify all potential applicants of the potential effect of a criminal record history on the recruitment and selection process and any recruitment decision.
- Discuss the content of the disclosure with the applicant before withdrawing an offer of employment.
- Make every subject of a disclosure aware of the existence of this Code of Practice and make a copy available on request.
- Have a written policy on the suitability of ex-offenders in relevant positions. This should be available on request to potential applicants.

4. Handling of disclosure information

Recipients of disclosure information (electronic or other means including update service information)

- Have a written policy on the secure handling of information provided by DBS, electronically or otherwise), and make it available to individuals at the point of asking them to complete a DBS application form or asking consent to use their information to access any service DBS provides.
- Handle all DBS related information provided to them by their employee or potential employee in line with obligations under data protection legislation.
- Handle all information provided to them by DBS, as a consequence of applying for a DBS product, in line with the obligations under data protection legislation.
- Ensure that a result received as part of an application submitted electronically is not reproduced in such a way that it infers that it is a certificate issued by DBS.
- Ensure any third parties are aware of the data protection principles and provide them with guidance on secure handling and storage of information. For data protection purposes, information passed to a registered body by DBS remains the responsibility of the registered body even if passed to a third party.
- Ensure business continuity and disaster recovery measures are in place and comply with data protection requirements.
- Must comply with security requirements under data protection legislation.

Registered persons

- Must use all reasonable endeavours to ensure that they only submit criminal record check applications in accordance with the legislative provisions which provide eligibility criteria for relevant positions or employment.
- Must ensure that before allowing a DBS check application to be submitted, they have assessed the role to be eligible under current legislation, correctly applied the right level of check, and correctly requested the appropriate barring list information.
- Must ensure they are legally entitled to request any DBS product being applied for.

Assurance

Registered persons and those in receipt of update service information shall:

- Cooperate in full and in line with timescales in current procedures with requests from the DBS to undertake assurance checks in relation to on-going compliance of registered bodies and those in receipt of update service information.
- Implement the suspension or de-registration of a registered body where non-compliance is established in line with current procedures.

5. Failure to comply with the conditions of registration

Recipients of disclosure information, through electronic means or via the applicant's copy of the disclosure, must note that 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. It is also an offence to:

- Disclose information to any member, officer or employee where it is not related to that employee's duties.
- Knowingly make a false statement for the purpose of obtaining, or enabling another person to obtain, a certificate.

Registered bodies and those in receipt of update service information believed to have committed an offence will be liable to prosecution, suspension or de-registration.

The DBS is empowered to suspend or cancel registration following a set legislative process with clear timescales if there is a failure to comply with the conditions of registration. Failure to comply with requirements set out in data protection legislation may also result in enforcement from the Information Commissioners Office (ICO).

6. University process for disclosures

Faculties and units who request disclosures for individuals should contact the People Hub on 01908 (5)41111, via Ask People Services or by emailing People-Hub@open.ac.uk.

7. Useful references

Recruitment of Ex-Offenders Policy
Data Protection Code of Practice