

Code of Practice

Introduction

The Disclosure and Barring Service (DBS) publish a guide for Registered Bodies and other recipients of disclosure information. This is an extract from these documents prepared by Care Admin for their customers.

For a full copy of the guide, see the DBS [website](#).

The code is intended to ensure that information released in disclosures is used fairly, and to provide assurance to applicants that this is the case.

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

The Code of Practice applies to all recipients of disclosure information. Where reference is made to employers, this should include employment agencies, voluntary organisations and those using the services of volunteers.

Obligations of the Code

Fair Use of Disclosure Information Recipients of disclosure information shall:

- Not unfairly discriminate against the applicant on the basis of conviction or other details revealed.
- Have a written policy on the recruitment of ex – offenders so that a copy can be provided to the applicant on request.
- Ensure that advertisements and applications forms contain a statement that a disclosure will be requested in the event of a successful application.
- Include a statement in application material to the effect that a criminal record will not necessarily be a bar to obtaining a position.
- Discuss any matters revealed in a disclosure with the person seeking the position before withdrawing an offer of employment.
- Make every applicant aware of the existence of the Code of Practice and make a copy available on request.

Handling of Disclosure Information Recipients of disclosure information:

- Must ensure that disclosure information is not passed to persons not involved in the recruitment decision. Unauthorised disclosure is a criminal offence. Emailed disclosure certificates must not be forwarded to any other individual, nor should more than one copy be printed.
- Must securely store disclosures and the information they contain.

- Should retain neither disclosures, nor the information they contain for longer than is necessary for the purpose it was obtained. In general, this should not be longer than six months after the date the recruitment decision was made.

Background and Types of Disclosures

Enhanced Disclosures

Enhanced disclosures are available for an individual whose job involves regular contact with young people under 18, or vulnerable adults. It also includes regularly working on premises principally used for young people or vulnerable adults. 'Regular' is defined as once a week or more frequently.

An enhanced disclosure will contain the same details as a standard disclosure. It also contains any information held about the applicant on the vetting and barring lists. These are lists of people considered unsuitable to work with vulnerable groups and are maintained by the DBS.

The enhanced disclosure may also contain non – conviction information from local police records which a chief police officer considers relevant to the position applied for.

Good Recruitment Practice

Good practice in recruitment is to make the best possible use of disclosure information. It is crucially important that people who have been convicted are treated fairly and are given every opportunity to establish their suitability for positions. The existence of a disclosure service should not be regarded as a substitute for any of the full range of pre – recruitment checks, including taking up references and enquiring into the person's previous employment history. Disclosures are complimentary to existing recruitment practice and should only be sought after an applicant has been provided with a conditional offer of employment.

Sensitivity of Disclosure Information

All information disclosed is sensitive personal information. All recipients of disclosure information must treat such information with care and responsibility.

Identity of the Applicant

It is good recruitment practice for employers to satisfy themselves as to the identity of the applicant, particularly in relation to posts involving contact with children or vulnerable adults. Such checks are also very helpful for the purposes of applying for a disclosure.

Please see the following ID Checking Guideline Links:

ID Checking Guidelines DBS: [Open](#)

All documents must be in the applicant's current name, and where an applicant has changed their name by marriage, deed poll or any other mechanism, the employer should see evidence of the change.

Overseas Applicants

Disclosure information is not available for foreign or UK nationals for any period they are resident outside the UK.

However a substantial period or overseas residence should not preclude employers from considering applicants with such backgrounds. The disclosure service should only be part of the overall recruitment process. In these situations employers should engage a full range of pre-employment checks beyond simple reference to disclosures.

Consideration of Disclosure Information

Factors to take into Account

Employers should take account of a number of factors before making a recruitment decision, viz:

- Whether the conviction or other matter is relevant to the position in question.
- The seriousness of the matter revealed (indicated by the sentence).
- The length of time since the offence occurred.
- Whether the applicant has a pattern of offending behaviour.
- Whether the applicant's circumstances have changed since the offending behaviour.
- The circumstances surrounding the offence and the explanation offered by the applicant.

Ultimately it is the responsibility of the employer to decide whether to offer the applicant a position. However, recruiters should be aware of their duties under the provisions of the Criminal Justice and Court Services Act 2000 which are:

- It is an offence to work with children (paid or unpaid) if disqualified from working with children. Disqualification arises from inclusion in the barred lists held by the DBS. In addition, courts can disqualify those convicted of serious offences from working with children. It is an offence to knowingly offer a disqualified person such work.

Validity

Disclosures do not have an expiry date because a conviction could be recorded against the applicant at any time after the disclosure is issued. Employers are advised to make a recruitment decision as soon as possible after a disclosure is issued.

Where an applicant disputes information provided in a disclosure, that dispute must be resolved before an employer can make a recruitment decision. If it should not prove possible to resolve a dispute by other means, a fingerprint check may be sought through DBS to determine whether the information provided relates to the applicant.

Handling Information

Security

Disclosure information must be kept securely and only those entitled to see it in the course of their duties may have access.

There may be circumstances where a recipient of disclosure information is asked to reveal details to a third party in connection with legal proceedings, e.g. an employment tribunal case. In such circumstances, the recipient of the information should inform the DBS of the request, and not reveal any information until advised by the DBS.

Storage

Disclosures should be kept in a locked, non-portable storage container. Keys or combinations for such storage units should not be freely available and access must be restricted to named individuals. E-Certificates must be stored in secure folders.

Retention of Disclosure information

Once a recruitment decision is made, the employer must not retain the disclosure for longer than necessary. In general, it should not be longer than 6 months. This period would allow for any disputes to be made and settled. Holding disclosures for longer periods may infringe the applicant's human rights, and data protection legislation may also be infringed. It is advisable to keep a record of the date of the disclosure, the unique disclosure number, the name of the applicant, and the type of disclosure. This is evidence that a disclosure was obtained.

Disclosures must be destroyed by secure means – i.e. deleting, shredding or pulping. They should not be kept in insecure waste receptacles whilst awaiting destruction.

No photocopies of disclosures may be retained, nor must any copy of the disclosures be made or kept. No more than one copy of an e-Certificate may be printed off.