



Home Office

Revised Code of Practice for Disclosure and Barring Service Registered Persons

November 2015

Revised Code of Practice for Disclosure and Barring Service Registered Persons

Presented to Parliament pursuant to section 122 (2) of the
Police Act 1997

November 2015



© Crown copyright 2015

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at samuel.wray@homeoffice.gsi.gov.uk

Print ISBN 9781474125512

Web ISBN 9781474125529

ID 23101511 11/15

Printed on paper containing 75% recycled fibre content minimum.

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

Contents

Introduction	3
Who does this Code apply to?	3
Disclosure Offences: Sections 123 and 124 of the Police Act 1997	3
What happens if the Code is breached?	4
The Obligations	5
Registration Details	5
Application Process	5
Identity Verification	5
Data Handling	6
Suitability Policy	6
Payment of Fees	7
Eligibility	7
Compliance Requests	8
Glossary	9

Introduction

The Disclosure and Barring Service (DBS) was established in December 2012 under Part V of the Protection of Freedoms Act (POFA)¹ to undertake disclosure and barring functions. There are specific legal requirements around these checks. Disclosure functions are set out in Part V of the Police Act 1997,² which requires Registered Bodies to adhere to this Code of Practice.

Who does this Code apply to?

The Code of Practice applies to all Registered Bodies with the Disclosure and Barring 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. This includes those Registered Bodies that provide an umbrella function to non registered organisations. The Code refers to any information exchanged between DBS and the Registered Body.

The Code of Practice does not apply to other third parties. The DBS will seek to ensure compliance with the Code through the full range of DBS assurance management processes.

All applicants for a DBS check should be made aware of this Code of Practice and provided with a copy on request.

Disclosure Offences: Sections 123 and 124 of the Police Act 1997³

Although certificates are now 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 to them by their employees or applicants for posts, including volunteers.

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. Furthermore, it is also an offence to:

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

¹ <http://www.legislation.gov.uk/ukpga/2012/9/part/5/enacted>

² <http://www.legislation.gov.uk/ukpga/1997/50/part/V>

³ <http://www.legislation.gov.uk/ukpga/1997/50/section/124>

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.

What happens if the Code is breached?

The Police Act 1997 (Criminal Records) (Registration) Regulations 2006⁴ sets out Conditions of Registration. Regulation 7(h) is for compliance with the Code of Practice issued under section 122 of the Act.

Failure to comply with Conditions of Registration can result in the suspension or cancellation of registration. This follows a set legislative process with clear timescales.

Failure to comply with requirements set out in the Data Protection Act may also result in enforcement action from the Information Commissioner's Office (ICO).

⁴ <http://www.legislation.gov.uk/uksi/2006/750/contents/made>

The Obligations

Registration Details

The Police Act 1997 (Criminal Records) (Registration) Regulations 2006⁵ sets out the obligations a Registered Body must meet in order to retain its registration.

Registered Bodies must:

1. Provide up-to-date information to the DBS in respect of their registration information and counter signatories in line with current procedures.
2. Maintain all accounts, online or otherwise, for all DBS products and delete when no longer required.
3. Ensure any electronic system used complies with specifications set out in the above regulations.

Application Process

Registered Bodies must:

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

Identity Verification

Registered Bodies must:

1. Verify the identity of the applicant prior to the submission of an application for a DBS product by following the current guidelines issued by DBS.⁶
2. Ensure that any person undertaking identity verification checks on their behalf follows the current guidelines issued by DBS.
3. Make sure lead or counter signatories do not validate their own applications for any DBS products.

⁵ <http://www.legislation.gov.uk/uksi/2006/750/contents/made>

⁶ <https://www.gov.uk/disclosure-barring-service-check/documents-the-applicant-must-provide->

Data Handling

Failure to comply with DPA requirements could result in enforcement action from the ICO.

In line with the Data Protection Act 1998 Registered Bodies and those in receipt of Update Service information must:

1. 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 requesting them to complete a DBS application form or asking consent to use their information to access any service DBS provides.
2. 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 Act 1998.
3. Handle all DBS related information provided to them by their employee or potential employee in line with the obligations under Data Protection Act 1998.
4. 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.
5. 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.
6. Ensure business continuity and disaster recovery measures are in place and comply with Data Protection requirements.
7. Must comply with security requirements under principle 7 of the Data Protection Act.⁷

Suitability Policy

Registered Bodies and those in receipt of Update Service information must:

1. Have a written policy on the suitability of ex-offenders for employment in relevant positions. This should be available upon request to potential applicants and, in the case of those carrying out an umbrella function, should be made available to their clients. Clients of Registered Bodies should make this policy available to their potential or existing employees.
2. Ensure that all applicants for relevant positions or employment are notified in advance of the requirement for a Disclosure.
3. Notify all potential applicants of the potential effect of a criminal record history on the recruitment and selection process and any recruitment decision.
4. Discuss the content of the Disclosure with the applicant before withdrawing any offer of employment.

⁷ <https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/>

Payment of Fees

Registered Bodies must:

1. Pay all registration fees in line with time periods set out in current procedures.
2. Pay all fees relating to DBS products in line with time periods set out in current procedures.
3. Pay all fees related to criminal records check applications submitted after any decision by the DBS to suspend registration or deregister the organisation.
4. 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.
5. Publish all fees, in relevant documentation, associated with the processing of criminal records check applications when you do so on behalf of others.
6. Notify the DBS in writing of any change to the fees 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 1975.⁸
- 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.⁹
- Enhanced checks with children's and/or adults' barred list check(s) – 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).

Registered Bodies must:

1. Use all reasonable endeavours to ensure that they only submit Criminal Records check applications in accordance with the legislative provisions which provide eligibility criteria for relevant positions or employment.
2. 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.
3. Ensure they are legally entitled to request any DBS product being applied for.

⁸ <http://www.legislation.gov.uk/uksi/1975/1023/contents/made>

⁹ The various Police Act 1997 (Criminal Records) regulations can be found by searching on <http://www.legislation.gov.uk>

Compliance Requests

Registered Bodies and those in receipt of Update Service Information must co-operate in full and in line with the timescales in current procedures,¹⁰ when DBS enquiries are made in relation to:

1. Ongoing compliance of Registered Bodies and those in receipt of Update Service information with the obligations under this Code.
2. Implementing the suspension or de-registration of a Registered Body where non-compliance is established in line with current procedures.

¹⁰ Available at <http://www.gov.uk/DBS>

Glossary

Registered Body – employer or company registered with the DBS for the purposes of processing and submitting applications for DBS products.

Umbrella function – Registered Bodies processing and submitting applications for DBS products from employers not eligible to register with the DBS.

DBS Product – Any level of check available from DBS.

Client – Company or individual engaging umbrella functions from a registered body.

ISBN 978-1-4741-2551-2



9 781474 125512

Disclosure and Barring Service Standard/Enhanced Disclosure Applicants Privacy Policy

1. About us

- 1.1. The Disclosure and Barring Service (DBS) helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.
- 1.2. Every year we issue around four million Disclosure certificates. We also manage both the children's and adults' barred lists.
- 1.3. We search police records and in relevant cases, barred list information, and then issue a DBS certificate to you.
- 1.4. Occasionally, depending on circumstances, and in order to produce a complete and accurate certificate, we must issue a manually produced certificate. Manual certificates follow the same checking processes as our system-generated certificates and are equally valid. It must be noted however, that applicants issued with a manual certificate cannot join the update service with that certificate.
- 1.5. We know that information released on DBS certificates can be extremely sensitive and personal. Therefore, organisations using the DBS checking service must comply with our [code of practice](#). The code is there to ensure organisations are aware of their obligations and that the information released will be used fairly. The code also ensures that sensitive, personal information disclosed by the DBS, is handled and stored appropriately and is kept for only as long as necessary.
- 1.6. DBS offer different types of check issued under the Police Act 1997:
 - a basic check shows unspent convictions and conditional cautions under the terms of the Rehabilitation of Offenders Act 1974
 - a standard check shows spent and unspent convictions, cautions, reprimands and final warnings which are not subject to filtering
 - an enhanced check shows the same as a standard check plus any information held by local police that is considered reasonably relevant, and ought to be disclosed, relating to the child or adult workforces. Where the application is for any other role, the police will consider the nature of the role in the release of information
 - an enhanced check with barred lists shows the same as an enhanced check plus whether the applicant is in the list of people barred from doing the role
- 1.7. Employers can only carry out a standard or enhanced check when you apply for certain roles. For example you may be applying for a role in either healthcare or childcare.

1.8. You will have the ability to [track your application](#) for standard and enhanced checks. You will need to enter your form reference number and date of birth in order to use this facility.

2. What is it I need to know?

2.1. This is our Privacy Policy. It tells you how we will use and protect any information we hold about you as part of your standard or enhanced disclosure application.

2.2. The Policy also explains what your rights are as a standard or enhanced applicant under the General Data Protection Regulations. It says why we need your personal data, what we will do with it and what you can expect from us. It also explains how to get a copy of any personal data we may hold about you. This is called a [Subject Access Request](#).

2.3. We do have other Privacy Policies that cover our other statutory functions. They can be accessed [here](#).

3. How will we use the personal information supplied to us?

3.1. We at the DBS collect your personal data in order to:

- process requests for criminal records checks (DBS checks). This will include searching police records, issuing a DBS certificate to the applicant and in certain circumstances, obtaining fingerprints
- decide whether it is appropriate for a person to be placed on or removed from a barred list, if information is disclosed on a DBS certificate
- process 'Adult First' checks - this is a service provided by the DBS under the Police Act 1997. It can be used in exceptional cases where a person is permitted to start regulated activity work with adults, before a DBS certificate has been obtained. This service is only available to organisations who are eligible to access the DBS adults' barred list and who have requested a check of the barred list on their DBS application form. The DBS Adult First check allows an individual to be checked against the DBS adults' barred list ahead of the Disclosure certificate being issued. A preliminary result is sent to the Registered Body who submitted the application
- process payments when appropriate

3.2. The information we collect about you depends on the reason for your business with us. We may use the information we obtain for any of the purposes listed above.

3.3. Your information may also be used for testing purposes. Testing is undertaken to ensure that our systems function as per specified requirements. If it is not practical to disguise your data or use dummy data then we will test our system using your data. This testing will only take place in environments that are secured to the same level as our live system.

Please note we may use previous applications you have submitted to assist in the checking process.

4. Who is the data controller?

- 4.1. A data controller decides the purpose and the manner in which any personal data is processed.
- 4.2. The DBS is the data controller of information held by us for the purposes of GDPR. We are responsible for the safety and security of the data we hold.

5. Who are the data processors?

- 5.1. A data processor is anyone (other than an employee of a data controller) who processes that data on behalf of the controller.
- 5.2. At the DBS we have a range of suppliers who process data on behalf of DBS as defined in section 9. We make sure that our data processors comply with all relevant requirements under data protection legislation. This is defined in our contractual arrangements with them.

6. Contacting the Data Protection Officer

- 6.1. The DBS Data Protection Officer Elaine Carlyle can be contacted via telephone on **0151 676 1154**, via email at dbsdataprotection@dbs.gsi.gov.uk, or in writing to:

**Elaine Carlyle
DBS Data Protection Officer
Disclosure and Barring Service
PO Box 165
Liverpool
L69 3JD**

7. What are the legal grounds for processing my information?

- 7.1. The DBS was established under the Protection of Freedoms Act (PoFA) 2012 on 1 December 2012. Disclosure functions of the DBS are contained within Part V of the Police Act 1997.
- 7.2. We provide a service which enables employers in the public, private and voluntary sectors to make suitability decisions. We do this by providing information to enable them to determine whether individuals are unsuitable or unable to undertake certain work in particular, with occupations involving regular contact with vulnerable groups, including children.
- 7.3. In addition to the above, we may share information with third parties for other purposes where we are legally permitted to do so.

8. Why would DBS hold my personal data?

- 8.1. We will only hold your data if you have:
 - previously used or are using the Disclosure Service

DBS Standard/Enhanced Applicants Privacy Policy V1.0

- been referred to the DBS for consideration under the Safeguarding Vulnerable Groups Act 2006 (SVGA) or Safeguarding Vulnerable Groups (Northern Ireland) Order 2007
- been cautioned or convicted for a relevant (automatic barring) offence that leads to the DBS considering you for inclusion in one or both lists

8.2. If we ask you for personal information, we will:

- make sure you know why we need this information
- only ask for information that we need
- ensure only those appropriate have access to it
- store your information securely
- inform you if the information will be shared with a third party
- ask you to agree to us sharing your information where you have a choice
- only keep your information for as long as we need to – see our [Retention Policy](#)
- not make it available for commercial use (such as marketing) without your permission
- ensure you are provided with a copy of data we hold on you, on request – this is called a [Subject Access Request](#)
- ensure there are procedures in place for dealing promptly with any [disputes](#) or [complaints](#)

Please note: We will share information with 'relevant authorities' such as the police, government departments etc. under UK Data Protection Act Prevention and Detection of Crime (Sch2, Part 1 Paragraph 2).

We will also share information under UK Data Protection Act (Sch2 Part 2 Paragraph 5 (2)) where disclosures are required by law or made in connection with legal proceedings.

8.3. In return, we will ask you to:

- give us accurate information
- tell us as soon as possible if there are any [changes to your details, such as a new address](#)

8.4. This helps us to keep your information up to date and secure. It will apply if we hold your data on paper or in electronic form.

9. Organisations that are involved in the Disclosure Service

9.1. Data will be passed to organisations and data sources involved with the DBS where we are legally permitted to do so. This includes:

DBS Standard/Enhanced Applicants Privacy Policy V1.0

- Tata Consultancy Services (TCS) including their third party suppliers – a partner and data processor in the DBS service
- Police forces in England, Wales, Scotland, Northern Ireland, the Isle of Man, and the Channel Islands – searches will be made on the PNC and data may be passed to local police forces. The data will be used to update any personal data the police currently hold about you
- ACRO Criminal Records Office - manages criminal record information and improves the exchange of criminal records and biometric information
- Other data sources such as British Transport Police, the Service Police and the Ministry of Defence Police - searches are made using an internal database. Where a match occurs the information will be shared to ensure that the record match is you
- Disclosure Scotland – if you have spent any time in Scotland, your details may be referred to Disclosure Scotland
- Garda - if information held by Police Service Northern Ireland (PSNI) indicates some information exists in the Republic of Ireland your details may be referred to Garda
- Access Northern Ireland – if you have spent any time in Northern Ireland your details may be referred to Access Northern Ireland
- Independent monitor (IM) - to undertake reviews on local intelligence (approved information) released by local police forces
- Independent Complaints Reviewer (ICR) - part of their role to investigate complaints that have gone through internal review process
- United Kingdom Central Authority - for exchange of criminal records with other EU countries
- The Child Exploitation Online Protection Centre (CEOP) who are National Crime Agency (NCA) Command
- Registered Bodies – the bodies registered with the DBS to submit Disclosure checks
- DXC Technology - our provider for cloud storage
- ATOS - for the collection of e-bulk application data
- National Identity Services (NIS) – assisting in the uploading of old criminal records from Micro Fiche to the Police National Computer (PNC)

10. Where is my data stored?

- 10.1. Your data is held in secure paper and computer files. These have restricted access. Where your data is held in paper format we have secure storage and processes for this. In some cases we may use secure off-site storage. We have approved

measures in place to stop unlawful access and disclosure. All of our IT systems are subject to formal accreditation in line with Her Majesty Government (HMG) policy. They also comply with the security required within GDPR to make sure that personal data is processed in a manner that ensures appropriate security of the data including protection against unauthorised or unlawful processing.

11. How long will DBS hold my information?

11.1. We operate a [Data Retention Policy](#) to ensure that data is not held for longer than necessary. However at present, there is a restriction on the destruction of information due to the ongoing Independent Inquiry into Child Sexual Abuse. DBS are currently reassessing the retention requirements in light of this.

11.2. Any data we identify that could be called on by the inquiry will be retained until completion of the inquiry. At this point the information will be securely destroyed as soon as is practicable.

12. What are my rights? How will DBS protect them?

12.1. We are committed to protecting your rights under the GDPR.

12.1.1. Your right to be informed

This document provides you with information in relation to how your data is processed as a DBS applicant. This ensures that we are transparent with regards to what we will do with the information you supply to us on your standard or enhanced application.

12.1.2. Your right to access to your personal data held by the DBS - known as a Subject Access Request

You have the right to request a copy of the information we hold about you.

On receipt of a valid application we will tell you whether we hold any data about you and provide you with a copy. Further information on how to apply can be found [here](#).

12.1.3. Your right to request that information held is accurate. Can I update it?

If you think that the information held by us at the DBS is incorrect, you have the right to request that it is corrected. If you challenge the accuracy of data that was provided to us by a third party we will send your request for correction to that party for their consideration.

It is the duty of both you and the Registered Body, the organisation who verifies your identity, to ensure that the information you have submitted on your application form is accurate.

If you believe you have submitted an error on an application that is still in progress you will need to contact us immediately on **03000 200 190**.

If you wish to [dispute](#) information contained on a completed certificate you can raise a dispute by contacting us on **03000 200 190**.

Third parties can also dispute a DBS certificate if they have all the necessary certificate information:

- the applicant's name
- the applicant's date of birth
- the certificate number
- the issue date
- the applicant's address

Where this is the case the applicant will be notified by the DBS that a third party has raised a dispute.

Read our guidance on [GOV.UK](https://www.gov.uk) for more information about disputes.

12.1.4. **Your right to request erasure of your personal data**

In certain circumstances you have a right to have personal data held about you erased. At the DBS we will only do this if certain criteria are met. There are some circumstances where this cannot be done therefore we advise you to seek independent advice before submitting an application to us.

Any [requests for information to be erased](#) will be considered on a case-by-case basis.

There are some specific circumstances where the right to erasure does not apply and we may refuse your request.

12.1.5. **Your right to prevent DBS from processing information which is likely to cause you damage or distress**

You have the right to request restriction of processing where it has been established that one of the following applies:

- the accuracy of personal data is contested, during the period of rectification
- where processing is unlawful
- where an individual has requested it is retained to enable them to establish, exercise or defend legal claims
- pending verification of the outcome of the right to object
- where processing has been restricted

DBS customers can request restriction of processing for any of the above reasons until these are resolved. Should you wish to restrict processing you will need to call the DBS helpline on **03000 200 190**. Any requests to stop processing will be considered on a case-by-case basis.

12.1.6. **Right to receive an electronic copy of any information you have consented to be supplied to us - known as data portability**

You have the right, where this is technically feasible, to electronically receive any personal data you have provided to the DBS to process, on a [consent](#) basis.

Please note that basic, standard and enhanced certificates are processed under our legal obligation, under Part V of the Police Act 1997, and barring information is processed under the Safeguarding and Vulnerable Groups Act 2006. Therefore, this information falls outside of the right to data portability.

All [requests for portability](#) will be considered on a case-by-case basis.

12.1.7. You have the right to object to the processing of your information

Should you wish for the DBS to stop processing your application you will need to [withdraw the application](#).

12.1.8. You have rights relating to automated decisions being made about you

Our disclosure process is generally automated. However if the system identifies that there is potentially police information held about you, this is then sent to the relevant police force for consideration regarding information which may be disclosed on your certificate. This is not an automated process and involves the judgment of the Chief Officer.

You have the right to object to any automated decision making. It should be noted that you would need to inform us of this on submission of your application as the certificate can be issued quite quickly. Please contact the DBS helpline on **03000 200 190**.

Barring service

The only automated decision process currently undertaken is for auto inclusion on a barred list without representations. On notification of inclusion on a barred list you will be informed if your decision has been made by automated means and you will be provided with the opportunity to request a manual review of this decision.

DBS do not currently undertake any profiling activities.

12.1.9. You have the right to make a complaint to the DBS and the Information Commissioner's Office (ICO)

If you wish to make a complaint to us regarding the way in which we have processed your personal data you can make a complaint to the Data Protection Officer via the contact details in [Section 6.1](#).

If you then remain dissatisfied with the response received, you have the right to lodge a complaint to the ICO at the following address:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

<https://ico.org.uk/>

13. Restrictions

13.1 There are restrictions to the rights of individuals and these are:

- National Security
- Defence Public Security
- Crime & Taxation

These restrictions are covered in more detail in the forthcoming Data Protection Bill 2018.

14. Transfer outside the European Economic Area

- 14.1 If you have spent time in the Channel Islands or the Isle of Man, it is likely that your data will be passed to police forces in that area. If any of your data has to be transferred outside of the UK, the DBS will ensure that an adequate level of protection is put in place.

15. Our staff and systems

- 15.1 All of our staff, suppliers and contractors are security vetted by the Home Office Security Unit prior to taking up employment. All staff are data protection trained and are aware of their data protection responsibilities. This is refreshed on an annual basis.
- 15.2 We conduct regular compliance checks on all DBS departments and systems. All checks are to the standard set out by the Information Commissioner's Office. In addition continual security checks are carried out on our IT systems.

16. Notification of changes

- 16.1 If we decide to change our Privacy Policy, we will add a new version to our website.