

Disclosure and Barring Service Subject Access Request 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.

2. About this policy

- 2.1.** The General Data Protection Regulation (GDPR) allows you to make a request to DBS for copies of all personal information we hold about you. This is known as a [Subject Access Request](#).
- 2.2.** This Privacy Policy applies to all individuals who make a subject access request to DBS, unless otherwise stated.
- 2.3.** The policy tells you what your rights are as an individual when requesting a copy of all the information that the DBS holds under GDPR Article 15, why we need to verify your identity, what we will do with it and what you can expect from us. It also tells you how to get a copy of any personal information we may hold about you. This is called, as mentioned above, a [Subject Access Request](#). There are further DBS privacy policies which cover our other statutory functions undertaken by DBS. They can be accessed [here](#).

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

- 3.1.** We will verify your identity to process a subject access request in order to:
- search our systems and clerical records to identify any information we may hold about you
 - prepare the information to be sent to you. This will be information already held. We will not reprocess your information to create any new records or products

4. Why would DBS hold my personal information?

- 4.1.** The most common reasons that we will hold your information is if you have:
- previously used or are using a Disclosure service to obtain a DBS certificate
 - been referred to DBS for consideration under the Safeguarding Vulnerable Groups Act 2006 (SVGA) / Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 (SVGO)
 - been included as a named victim or witness in a barring referral (you will need to tell us the name of the individual referred)
 - been cautioned or convicted for a relevant automatic barring offence that leads to DBS considering you for inclusion in one or both lists

- previously applied or are in the process of applying to be a Lead or Counter signatory of an organisation registered with DBS to process standard and enhanced applications
- previously applied or are in the process of applying to be an accountable officer within a responsible organisation set up to submit basic applications
- are or have been an employee of the DBS, Criminal Records Bureau or Independent Safeguarding Authority
- been involved in carrying out finance related functions for organisations who use our service
- been involved in delivering services via a contract

This is not a limited set of circumstances and we will search all our systems and records to check for information for all subject access requests.

5 Who is the data controller?

- 5.1 DBS is the data controller of information held by DBS for the purposes of GDPR. A data controller determines the purposes for which, and the manner in which, any personal data is to be processed (either alone or jointly or in common with others).
- 5.2 We have the responsibility for the safety and security of all the data we hold.

6 Who are the data processors?

- 6.1 Any supplier that works on behalf of DBS is one of our data processors. A data processor is any organisation that processes data on behalf of DBS. We make sure that our data processors comply with all relevant requirements under data protection legislation. This is defined in the contractual arrangements.

7 Contacting the Data Protection Officer

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

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

8 What can you expect from us?

- 8.1 We aim to provide you with a copy of the information we hold about you within one calendar month of receiving a valid request.
- 8.2 In rare circumstances where we cannot meet that deadline, we will contact you within that calendar month to tell you the reasons why and give you a realistic date of when we will provide the information. This should be no longer than 3 months from the original date of a valid application.
- 8.3 We will send you a copy of all the information we hold on you. Any third party information will be redacted unless we have consent from the third party to provide it.

- 8.4 We reserve the right to charge an administrative fee and will inform you of this.
- 8.5 Where possible, we will provide your information electronically if you wish. Please tell us if you want the information electronically.

9. What can you do if you think the information DBS holds is inaccurate?

- 9.1 If you are dissatisfied with the way your subject access request has been processed raise a concern with the DBS Data Protection Officer using the contact details at [7.1](#).
- 9.2 If you believe that data contained in your subject access information is incorrect, please complete the form that was in your subject access package and return it to the DBS.
- 9.3 If you believe that information contained on the print out of your disclosure related information is incorrect, you should raise a dispute rather than a concern. Please see guidance on raising a dispute [here](#).
- 9.4 If you wish to challenge information held on the barring referral, contact us on 03000 200 190.
- 9.5 Where the barring referral information was provided to DBS by another party this request will be forwarded to the relevant originating party and you should contact them direct. They will be asked to consider the request to correct the information e.g. if your request relates to an employer statement, strategy minutes or the PNC.

10. Who will we share your subject access request information with?

- 10.1 We will only share your information with a third party if you write to us and give your [consent](#) for us to provide it to someone else.

11. Where is my subject access stored?

- 11.1 Your information is held in secure paper and computer files, which have restricted access. Where your information is held in paper format we have secure on site storage and processes for this. All our IT systems are subject to formal accreditation in line with Her Majesty's Government (HMG) policy. They also align with the security required within GDPR to protect against unauthorised and/or unlawful processing.

12. How long will DBS retain my subject access information?

- 12.1 We operate a [Data Retention Policy](#) to ensure that information is not held for longer than necessary. Your subject access request and paperwork will be destroyed after six months. Information that populated the subject access paperwork however will be held on the original system or in clerical files for the time determined in our Data Retention Policy.
- 12.2 The Home Office has placed a restriction on the destruction of information due to the ongoing Independent Inquiry into Child Sexual Abuse (IICSA). To comply with DBS Data Retention Policy and the restriction, the DBS have agreed with the Information Commissioner's Office (ICO) to mark relevant information for secure destruction and place this information outside of operational control. It will only be supplied to IICSA following a legal request.

13. Our staff and systems

- 13.1 All our staff, suppliers and contractors are security vetted by the Home Office security unit before taking up employment. All staff are data protection trained and are aware of their data protection responsibilities. This is refreshed on an annual basis. We conduct regular compliance checks on all DBS departments and systems and continual security checks on our IT systems are undertaken.

14. You have the right to make a complaint to the DBS and the ICO

- 14.1 If you wish to make a complaint to DBS about the way in which we have processed your personal information you can make a complaint to the Data Protection Officer via the contact details in [Section 7](#). If you 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/>

15. Notification of changes

- 15.1. If we decide to change our privacy policy, we will add a new version to our website.