Disclosure and Barring Service
Data Retention Policy

Policy Reference Num.	DBS Retention Policy
Date of Implementation	01/06/18
Policy Owner	Elaine Carlyle
Policy Author	Michelle Anderson
Version	V7.0
Review Date	June 2019

Contents

1.0. Policy Statement

1.1 The Disclosure and Barring Service (DBS) is responsible for creating, maintaining and implementing legislative retention periods. The DBS is also responsible for implanting retention criteria for its own information records and ensuring compliance with the General Data Protection Regulation (GDPR).

1.2 This document sets out the DBS policy for the disposal and retention of records. It applies to all records, both in paper and electronic form.

1.3 The Home Office has placed an embargo on the destruction of information due to the ongoing Independent Inquiry into Child Sexual Abuse (IICSA). To comply with the DBS Data Retention Policy and the embargo, 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.

1.4 At the conclusion of IICSA and/or lifting of the embargo by the Home Office this information will be securely destroyed as soon as is practicable.

1.5 The data retention process **identifying** information for destruction on barring cases is still continuing and the information placed for destruction is put outside of operational control records and information.

2.0 Scope

2.1 This policy is intended for both DBS customers and staff and aims to provide an overview of the DBS Data Retention Policy. Further detailed instructions and schedules relating to the application of data retention are held internally by DBS.

2.2 Further information on general government record appraisal, selection and disposal can be found in the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act (FOI) 2000.

The Code sets out that under FOI, the disposal of records is undertaken in accordance with clearly established policies.

3.0 Principles

3.1 One of the main aims of successful record management is to be able to find, quickly and readily, any information requested. The FOI Act in January 2005 reinforced the need to know what

information we hold and to be able to locate it promptly and in compliance with GDPR.

3.2 The DBS will review information regularly to ensure that it is:

- **necessary** - the information must hold some value for the DBS to carry out its functions
- **proportionate** - in order to justify the retention of the information, it must be proportionate to retain the information against the impact on an individual's Human Rights - specifically in Human Rights Act Article 6, Right to a Fair Trial and Article 8, Right to Respect for Private and Family Life
- **adequate** - in order to justify the retention of information, it must be as complete as possible
- **relevant** - information must be fit for the purpose for which it is held
- **accurate and up-to-date** - all record details must be accurate, records must be updated with any new information
- **of historical value** - it may also be necessary to retain information of particular legal or historical significance. This relates to past-periods data, used usually as a basis for forecasting the future data or trends. From a DBS perspective papers relating to the setting up of CRB/ISA and subsequently DBS, would fall into this category

3.3 Factors which may impact on the retention of information are:

- **the age of information** - as time progresses information can become increasingly inaccurate
- **the reliability of information** - may be questioned/unreliable where the information is unproven
- **the reliability of the source of information** - sources of information may prove to be unreliable or false allegations may be made
- **social change** - changes in social acceptability of actions by individuals
- **legal requirement** - there may be a legal requirement to retain information for a specified period of time

4.0 What it means in practice?

4.1 The relevant owners of the documentation as detailed in the schedules within DBS are responsible for its review, in line with this policy and further detailed schedules. This applies to both electronic and paper records.

4.2 When the retention target is reached, the information will be reviewed to confirm that the information is to be further retained or destroyed. It will be destroyed if there is no further business, statutory or historical reason to keep them or to select them for re-review at a later date; either because the business need is ongoing or because of potential historical value.

5.0 Disclosure Applicants

5.1 Applicant Personal Data

Data Category	Retention Period	Notes
Data Applicant personal data record. **Criteria** All disclosure applications, this includes completed Disclosures Certificates in addition to those that are only partially completed if withdrawn or processing is stopped for any other reason. **Content** The deleted data will include all nominal (personal) data which can positively identify an applicant. This includes the data taken from the original application form, notes, disclosure details, service requests and any related inbound or outbound white mail. It will also include the image of the original individual application form plus the image of the disclosure certificate.	**CLEAR DISCLOSURES** Delete after **7 years** from the date of issue of the disclosure certificate, or from a cancellation or withdrawal of the disclosure application. **DISCLOSURES CONTAINING SOME FORM OF INFORMATION** Delete after **15 years** from the date of issue of the disclosure certificate, or from a cancellation or withdrawal of the disclosure application	Anonymised data should be retained for current MI purposes and can be held for as long as operational requirements dictate and for future MI reporting. This anonymised data will be categories such as age profiles, regions, type of employer, etc and will not identify individual applicants.

5.2 Update Service Registered Applicant Personal Data

Data category	Retention period	Notes
Data Applicant personal data record **currently registered** under the Update Service. **Criteria** Currently registered **Content** Includes all personal and audit data relating to the registrant.	Retain all data for the lifetime of the current registration.	Anonymised data should be available for current MI reporting purposes. This anonymised data will be categories such as age profiles, regions, type of employer, etc and will not identify individual applicants.

5.3 Manual Certificates

5.3.1 The Manual Certificate process is a contingency process which is used when a system based certificate is not possible. Information is retained in hard copies for certificates issued up to 2011 and records are kept electronically for all subsequent manual certificates and are subject to the same retention periods as electronic certificates.

5.4 Telephone Recordings – four years from the date the call was made

5.4.1 There are a number of telephone lines within DBS that are recorded and a message is played to DBS customers to advise them that the call is being recorded. The majority of telephone lines are not recorded. Where calls are recorded the recordings will be kept for four years.

6.0 Barring Operational Data

Document Type	Retention Period
Bar Information - Case Files System Record (see 6.10.3 for mandatory information that must be kept) **This category of information possesses the highest possible risk of harm to the public and in compliance with SVGA 2006 Regulations 2008/16.**	Retain for life of bar plus 10 years or until the individual has reached 100 years of age (whichever is sooner). Review every 10 years to ensure adequacy, relevance and necessity of retaining information.
General Team Information Minutes of meetings contact information	12 months delete
Policies/Procedures-	Delete 10 years after superseded
Non Bar Decisions - Case Files uCRM Record **This category of information may be used to indicate patterns of behaviour which are not proven or immediately obvious in the initial referral.**	Review after 5 years for low level allegations Stage 1 - Complete Disposal Stage 2B - 5 year Stage 2 - 10 year Review after 10 year clear period for all other types of cases. Destroy if review cannot justify the continued retention of the information.
Review / Appeals – DBS Barring Decision Upheld	See Adult & Child Bar Information above
Review / Appeals – DBS Barring Decision Not Upheld	See Non Bar Decisions (Adult & Child) above
Deceased Cases	Destroy 7 years after confirmation of Death is received

7.0 SVGA 2006 (barred List Prescribed Information) Regulations 2008/16

7.1 The SVGA (BLPI) regs 2008/16 sets out that information that DBS must keep in respect of an individual who is included in a barred list.

- Other information DBS must keep in respect of an individual included in a barred list.
- The descriptions of information set out in regulations 3 and 4 are prescribed as other information that the DBS must keep in respect of an individual who is included on a barred list.

7.2 Regulation 3

7.2.1 The information prescribed by this regulation is the following information related to the identity of the individual and provided to the DBS:

(a) any alternative names and aliases of the individual;

(b) the individual's date and place of birth;

(c) the address of the individual;

(d) & (e) removed by POFA

(f) the Police National Computer identification number relating to the individual;

(g) the criminal record certificate number relating to the individual;

(h) the national insurance number of the individual; and

(i) all additional information relating to the identity of the individual.

7.3 Regulation 4

7.3.1 The information prescribed by this regulation is the following information related to the DBS's functions:

(a) the date of the individual's inclusion on the barred list;

(b) all information provided to the DBS which it considers relevant to the decision of whether or

not the individual should be barred;

(c) any information provided to the DBS by keepers of relevant registers or supervisory authorities in accordance with sections 41 (Registers: power to refer) and 45 (Supervisory authorities: power to refer) of the Safeguarding Vulnerable Groups Act 2006;

(d) relevant police information provided to the DBS but which the DBS must not take account of for the purpose of deciding whether or not the individual should be barred, in accordance with paragraph 19(5) and (6) to Schedule 3 of the Safeguarding Vulnerable Groups Act 2006 (information which the chief officer of a relevant police force thinks that it would not be in the interests of the prevention or detection of crime to disclose to the individual);

(e) the reasons for the DBS's decision to bar the individual, including any findings of fact made by the DBS giving rise to that decision;

(f) any information provided to the DBS, including representations made to it by the individual, which the DBS considers might be relevant to any subsequent appeal or review; and

(g) the outcome of any such appeal or review and any information provided to or held by the DBS following such proceedings, including any findings of fact.

8.0 Abbreviations

DBS	Disclosure & Barring Service
DIT	Disclosure Information Team
DMU	Decision Making Unit
FOI	Freedom of Information
HO	Home Office
IICSA	Independent Inquiry Child Sexual Abuse