Disclosure &
Barring Service

Data Sharing Policy

VERSION 3.0

Data Sharing Policy

Version 3.0

Policy Reference Num.	Insert policy ref. no.
Date of Implementation	1 January 2017
Policy Owner	Elaine Carlyle / Head of Security and Facilities
Policy Author	Billy Machekano
Version	Version 3.0
Review Date	January , 2018

Contents

1.0 Policy overview

1.1. This document defines the policy governing activities whereby the Disclosure and Barring Service (DBS) data is shared with other bodies.

2.0. Scope

2.1. This policy applies to the management of data shared by DBS staff including contractors.

2.2. Third parties and Partners with whom DBS data is shared must observe DBS's procedures for protecting information.

3.0. The Policy

3.1. To comply with the requirements of this policy; you must ensure that:

a) No data sharing must take place before a successful completion of a Data Sharing Toolkit (DST) on any new data sharing arrangement. This includes the process to get it signed off by all relevant parties as indicated on the Toolkit. The Toolkit will determine if a Privacy Impact Assessment (PIA) is required; refer to Appendix B and C for further details. Existing MoUs will go through a transition period to ensure they comply with this policy.

b) The Data Sharing Toolkit and the Memorandum of Understanding (MoU) template must be completed by the member of staff arranging the data sharing, the Data Sharing Facilitator.

c) All data must be shared in accordance with the handling requirements determined by the classification and format of the data in accordance with DBS Media Policy arrangements.

d) Subject to any variation as laid down in (e) below; Data in any format must only be shared with the knowledge and permission of the Senior Information Risk Owner (SIRO) by following the governance process as outlined in (a) and (b) above.

e) Where the requirements laid out in this policy cannot be complied with or any amendments to the content of the MoU template are required (specifically information written in black) can only be permitted by following the variation process.

f) All MoUs must be signed by the SIRO. The SIRO is the final sign-off of all MoU and in his/her absence the Deputy SIRO.

g) Completion of the MoUs will be developed and managed from within the Business with assurance oversight from Data Protection Officer (DPO) and Information Governance Officer (IGO).

h) The DPO and IGO are members of the Data Sharing Forum which comprises of Strategy & Policy, Legal, Information Security and Information Asset Owners (IAO) who are also reviewers of the Data Sharing Toolkit during its approval process.

i) Access to shared sensitive assets must only be granted on the basis of a genuine need to know and an appropriate level of personnel security control.

j) Where commercial information is shared for business purposes; you must ensure the receiving party understands their obligations and protects the asset(s) according to its classification and in line with DBS information security requirements.

k) All data sharing activity must comply with the **Data Protection Act 1998.**

l) Any breach of this Data Sharing Policy not covered by a variation agreed by the SIRO must be reported as soon as it is discovered, and investigated in accordance with the DBS's investigations process.

m) All data incidents that might occur as a result of a data sharing agreement must be reported and follow the data breach procedure which can be found here.

n) All data sharing activities must be regularly assessed and where possible compliance audit carried out. This responsibility sits with the Data Sharing Governance team who will also maintain the centralised Data Sharing register of all approved MoUs, ensure quality control, and undertake compliance and assurance activities.

o) Compliance audits will be done on ad-hoc basis but regular quality control assessments/checks will be done at least annually for longer standing ongoing arrangements and more frequently for short lived arrangements.

p) Any data received by DBS from the other party must be handled in accordance of its classification and in line with the other party's requirements. Where the other party does not set any requirements, that data must be processed in compliance of the Data Protection Act 1998.

Appendix A – Policy Guidance Document

Contents:

1. Definitions of data sharing

Data sharing occurs when another body (for example; other Government Departments, Law Enforcement, Local Authorities, private organisations, foreign Governments or individuals) is provided with a copy of, or access to, data owned by DBS, or when DBS are provided with a copy of or access to data owned by another body.

2. Data Sharing Toolkit

All requests to share DBS data should be assessed using the Data Sharing Toolkit. This may include where data is shared and exchanged back and forth with a third party.

The Toolkit contains instructions for requesting sign-off from the appropriate authority. Further information regarding the Data Sharing Toolkit can be found in the Related Statements and Links section of this document.

As a rule, the majority of data that DBS share is personal data of which some of it will be of a sensitive nature and therefore all DBS data sharing will require an MoU with SIRO sign-off.

3. Data Protection Principles

All DBS data sharing must comply with the Data Protection Principles.

Principle 1: Personal data shall be processed fairly and lawfully

Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4 Personal data shall be accurate and, where necessary, kept up to date.

Principle 5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle 8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Consideration for sharing personal data

You should only consider applications for sharing personal information when they comply with the Data Protection Act 1998.

The management of any data sharing request should be taken forward in line with the specifications agreed in the toolkit and in line with the Data Protection Principles.

5. Consideration for sharing corporate data

The legislative landscape is less prescriptive in the case of corporate data and therefore the data sharing should be aligned with corporate and wider

government strategy. The data protection principles should be used as a guide to ensure that the corporate data sharing is done securely and that the sharing is legitimate.

6. Ongoing sharing

In the case of ongoing sharing DBS should assess the need for the arrangement at regular intervals. These intervals should be determined by a number of factors, including the regularity with which data is shared e.g. a weekly download would need more regular assessment than a yearly download. The focus of such reviews will be to ensure that they have remained: Justified; Proportionate; Necessary; Lawful; Secure. These key requirements should be used to decide whether the ongoing data sharing requires a more robust review, with an aim of potentially changing the scope of the sharing or even terminating it.

7. Handling Third Party Data

Where DBS process data shared by the other party; it is critical to consider the effect and impact to data subjects and to DBS's reputation, costs, etc if a security breach is to happen.

Ensure you take the following measures in respect of information that the other organisations share with you.

- Review what personal data you hold or have received from other organisations, making sure you know its origin and whether any conditions are attached to its use
- Indentify who has access to information that other organisations have shared with you; 'need to know' principles should be adopted.
- You should avoid giving all your staff access to shared information by other organisation if only a few of them need it to carry out their job in connection with the data sharing.

8. Information Asset Owners (IAO) responsibilities during data sharing

It is the responsibility of the IAO to

- ensure the toolkit is completed correctly
- ensure that all sharing carried out as a result of a process is logged, and that when a process is discontinued or replaced that it is recorded as such.
- ensure that the shared data is securely deleted in accordance with the data retention policy once the purpose of the sharing is fulfilled.
- ensure individuals' rights i.e. procedures for dealing with access requests, queries and complaints as a result of data sharing are dealt with in line with DBS subject access procedure.
- ensure that the information sharing agreement is complied with including the review of the effectiveness and termination of the sharing agreement
- Deal with any data breaches with support from Data Protection and Information Governance and Security teams.

9. Variations

The following processes are subject to a variation from this policy (this is not an exhaustive list and may be added to from time to time):

- Where there are interchange agreements or
- Where requests such as Court Orders or Independent Inquiries are made
- Pro-active provision of evidence to police to support prosecutions

10. Related statements and material

- PIA process – located *here*
- Data Sharing Toolkit – located *here (hyperlink)*
- MoU Template – located *here (hyperlink)*
- Data Sharing Variation Process – located *here (hyperlink)*