



Disclosure &  
Barring Service

## Data Sharing Agreement

between:

Disclosure and Barring Service and  
General Dental Council

## Table of Contents

List of Acronyms .....	3
Document Control .....	4
Form of Agreement .....	6
Part 1	
1. Introduction .....	7
2. Purpose of the Agreement.....	8
3. Governance, monitoring, amendment and termination of this agreement .....	9
4. Acknowledgements.....	10
Part 2	
5. Appendix 1: GDPR Principles .....	11
6. Appendix 2: Data Sharing Arrangements .....	12
7. Retention and Destruction .....	18
8. The Data Security and Assurance Procedure .....	18
9. Responsibilities and commitments of both parties to this agreement.....	22
10. Relationship Management.....	23
11. Signatories.....	25
12. Remarks.....	25

## List of Acronyms

CRB	Criminal Records Bureau
DBS	Disclosure and Barring Service
DPA	Data Protection Act 2018
DSA	Data Sharing Agreement
GDC	General Dental Council
GDPR	General Data Protection Regulation
IAO	Information Asset Owner
ICO	Information Commissioners Office
ISA	Independent Safeguarding Authority
NDPB	Non Departmental Public Body
PA	Police Act 1997
PNC	Police National Computer
POFA	Protection of Freedoms Act 2012
SIRO	Senior Information Risk Owner
SVGA	Safeguarding Vulnerable Groups Act 2006
SVGO	Safeguarding Vulnerable Groups (Northern Ireland) Order 2007

## Document Control

### REVISION HISTORY

Date	Comments	Author	Version
12/03/2018	Initial Draft	Lisa Grimstead Donna Sheehan	0.1
14/03/2018	Amendments made following review by Legal	Lisa Grimstead Donna Sheehan	0.2
04/04/2018	Amendments following first internal review	Donna Sheehan	0.3
27/04/2018	Amendments following approval from Head of Security	Donna Sheehan	0.4
22/05/2018	Amendments following second internal review	Donna Sheehan Lisa Grimstead	0.5
13/09/2018	Amendments made from external review	Donna Sheehan & Lisa Grimstead	0.6
03/10/2018	Amendments made following DBS response to GDC 2 <sup>nd</sup> review	Donna Sheehan	0.7
29/04/2019	Amendments made following 3 <sup>rd</sup> external review.	Donna Sheehan	0.8
08/05/2019	Amendments made following internal review by IGO and Legal	Donna Sheehan	0.9
23/05/2019	Baselined to version 1.0	Helen Parks	1.0

### REVIEWERS

THIS DOCUMENT HAS BEEN ISSUED TO THE FOLLOWING FOR REVIEW:

Name	Job role	Version
Karl Gergely	Information Asset Owner	0.7
Catherine Nicholas	Legal Representative	0.7
Clare Burrows	Legal Representative	0.8
Michelle Anderson	Information Governance Officer & Data Protection	0.8
David McLaren	Strategy & Policy	0.7
Stuart Mason	Assurance Manager	0.7
Donna Sheehan	DSA Officer	0.8
Helen Parks	DSA Lead	0.8
Barbara Moore	Team Leader	0.7
Rosemary Cairns	GDC Representative	0.9

## APPROVALS

THIS DOCUMENT WILL BE APPROVED BY THE SIRO

NAME	JOB ROLE	VERSION	APPROVED (Y/N)
PAUL WHITING	DEPUTY CHIEF EXECUTIVE & CHIEF FINANCIAL OFFICER (SIRO)	1.0	Y

**Part 1:**

*Form of Agreement*

This DATA SHARING AGREEMENT is made this 4 September 2019

Between

Disclosure and Barring Service (DBS) whose address is

Stephenson House, Alderman Best Way, Morton Palms Business Park,  
Darlington, County Durham, DL1 4WB

And

General Dental Council (GDC) whose address is

37 Wimpole Street, London, W1G 8DQ

## 1. Introduction

### DBS

- 1.1. The DBS is a Non-Departmental Public Body (NDPB) sponsored by the Home Office. It is established under the Protection of Freedoms Act 2012 (POFA) and carries out the functions previously undertaken by the Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA). The DBS helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.
- 1.2. It is responsible for:
  - 1.2.1. Processing criminal records checks (DBS checks).
  - 1.2.2. Placing in or removing people from the DBS children's barred list and adults' barred list for England, Wales and Northern Ireland (DBS Barred List's).
- 1.3. Information can be shared by and with the DBS under the provisions of relevant legislation including the Safeguarding Vulnerable Groups Act 2006 (SVGA), the Safeguarding Vulnerable Groups (Northern Ireland) Order (SVGO) and Part 5 of the Police Act 1997 (PA), as amended by the Protection of Freedoms Act 2012 (POFA), the Dentists Act 1984, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).
- 1.4. DBS operates a Privacy Policy which explains that personal information may be shared with a number of third parties including other government departments but will only be shared in accordance with relevant legislation.

### GDC

- 1.5. The General Dental Council is a statutory body independent of the NHS and of Government, with responsibility for maintaining the dentists' and dental care professionals' registers for the United Kingdom. The GDC aims to protect patients, promote confidence in dentists and dental care professionals and be at the forefront of healthcare regulation.

**1.6.** The GDC:

- 1.6.1 maintains registers of qualified dental professionals;
- 1.6.2 sets standards of dental practice and conduct;
- 1.6.3 assures the quality of dental education;
- 1.6.4 ensures dental professionals keep up to date;
- 1.6.5 helps patients with complaints about a dentist or a dental care professional; and
- 1.6.6 works to strengthen patient protection.

**1.7** The GDC has statutory powers to take action where there are concerns about the fitness to practise ('FtP') of a registered dentist or dental care professional. This includes those registrants whose fitness to practise is affected by their health.

**1.8** The GDC is also a Keeper of the Register under the SVGA.

## **2. Purpose of the Agreement**

**2.1.** This document is intended to act as an Agreement between the GDC and DBS. This is not a legally binding document but a process document that both parties will agree and abide to when sharing data. It is essential that all information shared under the terms of this Agreement will be done so in compliance with the key privacy legislation: GDPR, DPA, the Human Rights Act 1998, the Official Secrets Act 1989, and the Computer Misuse Act 1990.

**2.2.** It complements other agreements to which the parties may already be signatories and does not in any way supersede those existing agreements.

**2.3.** It is not intended that this Agreement be definitive or exhaustive, it is recognised that as policy develops and legislation changes this Agreement will need to be reviewed and amended in light of new data sharing requirements to ensure that it remains 'fit for purpose'.

**2.4.** This Agreement also aims to facilitate and govern the efficient, effective and secure sharing of good quality data between the parties.



**2.5.** This Agreement is comprised of two parts. Part 1 contains the **Form of Agreement**, and Part 2 contains the **Appendices**. The two are inseparable and shall form the entire Agreement.

**2.6.** Part 2 contains the following Appendices

<b>Appendix 1</b>	GDPR Principles
<b>Appendix 2</b>	<p><b>Data Sharing Arrangements:</b></p> <ul style="list-style-type: none"> <li>• Purpose for sharing data and the types of data being shared</li> <li>• Basis to which data sharing can be legally justified</li> <li>• The procedure for processing the data sharing</li> <li>• Retention and destruction</li> <li>• The Data Security and Assurance Procedure.</li> <li>• The responsibilities and commitments of both parties to this Agreement</li> <li>• Relationship management</li> </ul>

### **3. Governance, monitoring, amendment and termination of this agreement**

**3.1.** The governance and monitoring of this Agreement will be undertaken by DBS, and the GDC may also undertake reviews, if it wishes to (see under GDC heading in section 9 a. below). Formal reviews will be undertaken at least annually or at a shorter duration depending on the duration of the Agreement.

**3.2.** This Agreement can be amended or varied at any time in writing with the agreement within one month of both parties. The formal arrangements should be agreed and signed off by both parties' Senior Information Risk Owners (SIRO).

**3.3.** Either party may terminate this Agreement upon three months **written** notice to the other in the following circumstances.

- 3.3.1. by reason of cost, resources or other factors beyond the control of each party.
- 3.3.2. by reason of changes to legislation or policy dictating otherwise.
- 3.3.3. if any material change occurs which, in the opinion of either party following negotiation significantly impairs the value of the agreement to the parties in meeting their respective objectives; and,
- 3.3.4. in the event of noncompliance with the terms set out in this Agreement or a significant security breach that compromises the confidentiality or integrity of the personal data by either party. Termination of this Agreement does not affect the statutory obligations of each party.

## 4. Acknowledgements

### 4.1. Both parties acknowledge that:

- 4.1.1. They are subject to the Freedom of Information Act 2000 and to Subject Access requests under Article 15 of the GDPR. If either party receives a request they agree to co-operate with each other and where appropriate will consult with the other party before making a decision (subject to exemptions) to disclose information.
- 4.1.2. Data obtained by GDC from DBS or by using DBS systems or by any other means is subject to the [HMG Security Policy Framework](#) and GDC agree that it will be processed in accordance with similar security controls for example ISO27001 or equivalent. The HMG Security Policy Framework describes the standards, best-practice guidelines and approaches that are required to protect Government assets (people, information and infrastructure) which DBS is party to. It highlights expectations of how organisations and third parties handling Government information and other assets will apply protective security to ensure Government can function effectively, efficiently and securely.

4.1.3. DBS data carries an appropriate Government Security Classification with OFFICIAL as a minimum.

4.1.4. The processing of personal data will be done in compliance with the GDPR/DPA.

Both parties are Data Controller in their own right and therefore accepts that this Agreement treat them as such.

## Part 2: Appendices

### 5. Appendix 1: GDPR Principles

#### **Article 5 of the GDPR requires that personal data shall be:**

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability and governance is a legal requirement on data controllers who are responsible for compliance with the GDPR principles and must be able to demonstrate this to data subjects and the ICO.

## 6. Appendix 2: Data Sharing Arrangements

### 6.1. Purposes for sharing data and the nature of the data being shared

6.1.1 Notwithstanding section 1.3; information will also be shared for the purposes listed in 6.1.2 below that helps employers make safer recruitment decisions and helps regulators, such as the GDC, maintain their Registers of individuals who are able to work or volunteer in regulated activity, to prevent unsuitable people from working with vulnerable groups, including children.

#### 6.1.2 The purpose includes the following:

- a) In the interests of safeguarding vulnerable groups including children

#### 6.1.3 The benefits of the data sharing

- a) It assists the parties to fulfil their respective obligations under the SVGA and SVGO
- b) It provides DBS with information that will enable it to more effectively carry out its statutory duty to make barring decisions and in doing so, better safeguard vulnerable groups including children
- c) It assists GDC in the maintenance of the register of individuals who are able to work in regulated activity.
- d) It promotes co-operation between the parties at an operational level and in the conduct of their respective statutory duties
- e) It promotes consultation on matters of safeguarding to improve both parties' performance in meeting their respective statutory duties and corporate objectives.

#### The desired outcome for this data sharing is to:

- a) Improve awareness, intelligence analysis and dissemination capabilities that facilitates an effective and efficient sharing of information within existing legal powers and constraints concerning safeguarding vulnerable groups.
- b) clearly define information sharing requirements and promoting information management good practice

## 6.2 Nature of the Data being Shared

All **DBS** data shared will fall under the OFFICIAL classification as a minimum. This includes information which may be of a sensitive nature and deemed to be OFFICIAL-SENSITIVE.

### 6.2.1 The information type(s) that maybe shared and is determined on a case by case basis is information relating to:

#### From DBS to GDC

- Barred List status of an individual
- Data relating to individuals who are subject of a barring referral made by an employer or professional body.
- Copies of the relevant documents relating to the consideration bundle
- In cases where the DBS does not bar; if further information regarding the decision is available, and is not already included in the case documents, the DBS may provide a summary of the reasons not to bar on request.
- A copy of the Final Decision Letter.
- A summary of information from a Disclosure Information Print

#### From GDC to DBS

- Relevant information contained within a Fitness to Practise (FTP) Consideration Bundle
- Outcome decision(s) from Fitness to Practise cases. (The GDC may also provide information about other adverse fitness to practice history (i.e. below Practice Committee level cases) or complaints closed without action where relevant.)
- Information relating to an individual's status on GDC Register
- DBS Referral form from GDC including personal data and allegation information.

**6.2.2 The data fields of the information to be shared are:**

**From DBS to GDC**

- Title
- Full Name
- Alias Name(s)
- Siebel Case Reference number
- Registration Number
- Register Status
- Address(es)
- Date of Birth
- Alias date of Birth
- NINO
- Nationality
- Gender
- Qualifications
- Position held
- Education and Training
- Barred List Status

**From GDC to DBS**

- Title
- Full Name(s)
- Alias Name(s)
- Registration Number
- Register Status
- Address(es)
- Date of Birth
- Alias Date of Birth
- NINO
- Nationality
- Gender
- Qualifications
- Position held
- Education and Training

**6.2.3 The data source(s) for the data shared include**

**From DBS to GDC**

- Siebel
- Paper Case Files
- Employer Referral Information
- Professional Body Referral Information
- Disclosure Information Print

**From GDC to DBS**

- CRM System
- CARE System
- Employer Referral Information
- Paper Case Files
- Secure File Share

### **6.3 Basis upon which Data Sharing can be legally justified**

6.3.1. Both parties agree that they will comply with the GDPR Principles (Appendix 1) and will continue to do so when processing the shared data.

6.3.2. If information is found to be inaccurate, both parties will ensure that their records and systems are corrected accordingly

6.3.3. Each party has their own legal framework that enables them to share data. Both parties shall work together and share data to fulfil circumstances already identified in subsection 1.3 and 6.1.1.

6.3.4. **DBS:**

- **Provision of Barring Information**

Section 43 (3)(4) and (5) SVGA

Article 45 (3)(4) and (5) SVGO

- **Provision of Information for GDC Fitness to Practice cases**

Sections 33B and 36Y: Dentists Act 1984

- The parties acknowledge that there is the potential that the sharing of the information could constitute an interference with Article 8 of the European Convention on Human Rights as implemented into UK law by the Human Rights Act 1998 (that is, the right to respect for private and family life). However, as this is a qualified right, the parties acknowledge that any interference will need to be justified, necessary and proportionate. The sharing is undertaken in order to secure the protection of children and vulnerable adults. Both parties believe that the provision of information is necessary and proportionate, having regard to the purposes of the information sharing and the steps taken in respect of maintaining a high degree of security and confidentiality.

### 6.3.5 GDC:

- **Power to Refer**

Section 41 SVGA

Article 43 SVGO

- **Duty to Provide Information on Request**

Section 42 SVGA

Article 44 SVGO

- **Power to Share**

Section 33C and 36Z: Dentists Act 1984

- **Duty to Co-Operate**

Section 2A: Dentists Act 1984

- Legislation permits the sharing of information, which may include but not be limited to employers, other stakeholders, external law firms, the registrant themselves as required for the fulfilment of the roles and functions and carried out in the public interest.
- The information shared will be used and processed with regard to the rights and freedom enshrined within the European Convention on Human Rights. Both parties believe that the provision of information is necessary and proportionate, having regard to the purposes of the information sharing and the steps taken in respect of maintaining a high degree of security and confidentiality.

## 6.4. Procedure for the Data Sharing

6.4.1. A Data Sharing Toolkit and a Data Protection Impact Assessment have been completed by DBS prior to the commencement of the sharing to ensure compliance with the GDPR Principles.

### 6.4.2. From DBS to GDC

- a) Where DBS data will be shared to support GDC in maintaining the Register of individuals who are able to work or volunteer in



regulated activity, the GDC will make the request in writing e.g. by completing a Data Request Form.

- b) DBS will complete a Data Sharing Toolkit and follow its internal approval process to approve the request.
- c) DBS draft a DSA. The DSA should be signed off by the DBS SIRO and the GDC SIRO.
- d) Once the Data Sharing request is approved, DBS will extract the data set requested in line with its internal process guidelines.
- e) The volumes of data shared may vary and will be responded to on an ad hoc basis
- f) GDC will protect and store the data within a Customer Relationship Management system which is accessed and used in line with the GDPR principles and in line with the GDC's information governance policy framework and the SOPs supporting this data sharing Agreement.
- g) The method of Data Transfer between the two organisations will be via secure postal mail or secure electronic transfer. Information will be double bagged, if postal, and DBS use a secure government email address e.g. [dbsdspatch@dbs.gov.uk](mailto:dbsdspatch@dbs.gov.uk) (The gsi email domain has been replaced with the secure government gov.uk domain).
- h) GDC's Registration Operations team, Fitness to Practice staff in the Initial Assessment and Casework teams, staff in the GDC In-house Presentation Service (ILPS) and any external law firm or barrister instructed by the GDC to handle a particular case that involves data provided by DBS will have access to DBS data to carry out the activities agreed in this Agreement.
- i) GDC will process and handle the data in compliance with the GDPR/DPA and in line with its own policies and procedures and with the DBS Data Security and Assurance procedure (see section 8 below for more details).

#### 6.4.3 From GDC to DBS

- a) Where DBS considers that GDC data is needed to support DBS in carrying out its statutory safeguarding functions, the DBS will make a request in writing e.g. by letter to the named GDC contact identified in section 10.1 of this Agreement.
- b) Once the request for data has been verified as being genuine, GDC will extract relevant data from its Customer Relationship Management system in response to the request in line with its internal process, which usually involves a Senior Fitness to Practise Lawyer drafting a response for the Head of FtP Case Progression

with support, as necessary, from the Information Governance Team.

- c) The volumes of data shared may vary according to the data held in each individual case and will be responded to on a case by case basis.
- d) DBS will protect and store the data within their IT system which is accessed and used in line with the GDPR principles and in line with the DBS' information governance policy framework and the DBS processes supporting this data sharing Agreement.
- e) GDC will respond to data requests from DBS via its secure email facility known as GDC Secure File Share to a DBS secure email address e.g. dbdispatch@dbs.gov.uk.
- f) Relevant DBS staff only will have access to GDC data to carry out the activities specified in this Agreement.
- g) DBS will process and handle the data in compliance with the GDPR and in line with the DBS Data Security and Assurance procedure (see section 8 below for more details).

## 7. Retention and Destruction

- 7.1. Both parties will ensure that the data shared will not be kept for longer than is necessary for the purposes set out in this Agreement. However, at present, the Home Office has placed a moratorium on the destruction of information by DBS due to the ongoing Independent Inquiry into Child Sexual Abuse (IICSA) At the conclusion of the enquiries and/or lifting of the embargo by Home Office information will be securely destroyed as soon as is practicable. Information held by the GDC will be retained for the relevant period recorded in the GDC's corporate Retention Schedule and, thereafter, disposed of securely.
- 7.2. Once the information is no longer relevant for those purposes it will be securely destroyed in accordance within the guidelines of Infosec Standard No.5 (Issue No. 4 April 2011)

## 8. The Data Security and Assurance Procedure

- 8.1. Each party acknowledges that the other party places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the other party's location systems and procedures. Each party also acknowledges the requirement to maintain the confidentiality of data provided to it by the other party.

8.2. Each party shall be responsible for the security of its system and shall at all times provide a level of security which:

- Is in accordance with Good Industry Practice such as ISO27001, the HMG Security Policy Framework (SPF) [www.cabinetoffice.gov.uk/spf](http://www.cabinetoffice.gov.uk/spf) and related standards and Law. The SPF is for government departments and public services. Partners that don't follow the SPF should adhere to the ISO 27001 or equivalent as the minimum level required for security management;
- Is commensurate with the threats to its system.

8.3. Notwithstanding the above each party shall at all times ensure that the level of security employed in accessing data provided to it by the other party is appropriate to manage the risks associated with the following:

- loss of confidentiality, integrity and availability of such data;
- unauthorised access to, use of, or interference with such data by any person or organisation; and
- use of its system by any third party in order to gain unauthorised access to any computer resource or such data.

8.4. Both parties shall comply with any security operating procedures as detailed in this section 8 or instructions provided by the other party, and any further standards, guidance and policies and any successor to or replacement for such standards, guidance and policies, as notified from time to time.

8.5. In receiving data from the other party, each party agrees to:

- a) Ensure that there are adequate protective security measures in place to ensure the safeguarding of the storage, transmission or processing of data supplied by the other party;
- b) Each party shall limit access to data supplied by the other party to those persons required to carry out functions under this written Agreement (which, for the avoidance of doubt, includes external solicitors and barristers acting for the GDC in fitness to practise cases), save for where onward transmission is consistent with statutory or common law powers,

in which case the prior agreement of the party who supplied the data must be sought;

- c) Ensure any actions taken in respect of data provided by the other party are in accordance with all appropriate privacy legislations indicated in subsection 2.1;
  - d) Ensure that data provided by the other party is protected from unauthorised dissemination, and unauthorised or unlawful processing, and against accidental loss or destruction of, or damage to, personal data.
  - e) Obtain permission from the other party should data provided by that party be required for testing purposes.
- 8.6. In the event of paragraph 8.5(d) occurring, each party will inform the other as soon as possible (using contacts listed on section 10 of this document) and within 48 hrs of becoming aware of any data breach involving data that has been supplied to it by the other party. The party that becomes aware of the breach will follow its formal data breach incident management process, including reporting the breach to the ICO (where appropriate) within 72 hours of becoming aware of it.
- 8.7. Each party will have in place procedures or processes to minimise the risk of unlawful extraction of data provided by the other party under this Agreement including the control of removable media and data storage devices as required.
- 8.8. Each party will ensure that all of its staff including contractors with access to personal data, special category data and data relating to criminal convictions and offences, as defined in GDPR, supplied by the other party:
- a) have undergone background verification checks and/or satisfactory reference checks
  - b) are trained in the safeguards required to protect such data and in the restrictions on the use and dissemination of such data
  - c) are only allowed access to systems or services that process such data from the party's approved devices
- 8.9. Each party will ensure that there is auditable evidence that such safeguards are being applied.

8.10. Each party will ensure that there are robust processes in place to manage segregation of duties and remove access for those no longer requiring access to data supplied by the other party.

8.11. Where the conditions of the data processing change including in those circumstances listed below, each party must notify the other without delay:

- a) Any situation where the data processing is being off-shored outside of the UK or is being done in the Cloud;
- b) Any situation that disrupts the intended transfer of information to the other party;
- c) If it appears that any appropriate electronic, physical and /or procedural safeguards may or have been compromised, or;
- d) If it becomes aware of any attempt to affect such compromise in respect of any data supplied by the other party.

8.12. Each party will take appropriate action, in the event of misuse, unauthorised alteration, deletion of or access to or dissemination of data by its staff including Contractors or any third party.

8.13. Each party will inform the other immediately and subsequently delete any information received from the other which is not required for the data sharing.

8.14. Each party will have a written contract with any contractor it uses to carry out functions on its behalf, notified to the other party in advance of the commencement of that contract. Each party will ensure that:

- a) its system is assessed for information risk and provides adequate controls for processing the others' data;
- b) all access to the other party's data on the other party's system is controlled and limited to individuals who have undergone employee background verification checks and/or satisfactory reference checks and that all such access is logged and monitored, and that any irregularities of access are reported immediately to the other party and investigated.

## 9. Responsibilities and commitments of both parties to this agreement

### DBS

- a. DBS may have the right to Audit; to ensure all aspects of this agreement are adhered to and quality control measures are implemented. This may be done through regular assessments mechanisms which may include the use of questionnaires.
- b. Ensure at all times when providing and sharing data that the data is relevant, accurate and up-to-date.
- c. DBS ensure that data is transferred to the Data Recipient securely in accordance of its classification.
- d. DBS to ensure all aspects of this Agreement are adhered to.
- e. DBS to ensure staff handles data in line with the approved secure transfer method agreed by both parties and within the data security classification of those data and ensure retention policy and data destruction policy is adhered to.
- f. DBS to provide the information to the GDC in line with the procedure set out in this Agreement and via the relevant contacts provided in this Agreement as indicated in section 10 below.

### GDC

- a. GDC may have the right to Audit; to ensure all aspects of this Agreement are adhered to and quality control measures are implemented. This may be done through regular assessment mechanisms which may include the use of questionnaires.
- b. GDC to ensure all aspects of this Agreement are adhered to.
- c. Ensure at all times when providing and sharing data that the data is relevant, accurate and up-to-date.
- d. GDC to ensure that data is transferred to the DBS securely in accordance of its classification.
- e. GDC to ensure staff handle data in line with the approved secure transfer method agreed by both parties and within the data security classification (or equivalent) of those data and ensure retention policy and data destruction policy is adhered to.
- f. GDC to provide the information to the DBS in line with the procedure set out in this Agreement and via the relevant contacts provided in this Agreement as indicated in section 10 below.

## 10. Relationship Management

### 10.1. Day to Day Management

The day to day management of this Agreement by DBS and the GDC will be undertaken by:

Organi sation	Job Title	Name	Email	Phone
DBS	IAO	Karl Gergely	gergely.karl@dbs.gov.uk	01325 953538
GDC	Executive Director, Fitness to Practise Transition	Tom Scott	tscott@gdc-uk.org	0207 1676209

### 10.2. Business Contacts

The Business contacts of this Agreement are:

Organisation	Role	Name	Email	Phone
DBS	Data Protection Officer	Elaine Carlyle	elaine.carlyle@dbs.gov.uk	0151 6761559
DBS	Information Governance & Security Manager	Michelle Anderson	michelle.anderson3@dbs.gov.uk	01325 953602
DBS	Relationship Management	Stuart Mason	stuart.mason@dbs.gov.uk	01325 953839
DBS	Freedom of Information	Christine Burls	dbsfoi@dbs.gov.uk	
DBS	Operational Contact	Barbara Moore	barbara.moore@dbs.gov.uk	01325 953533

GDC	Data Protection Officer	Luke Whiting	dpo@gdc-uk.org	0207167 6309
GDC	Relationship Management	Clare Callan, Head of FtP Case Progression  Jonathan Meadows, Head of In- house Legal Presentation Service	ccallan@gdc-uk.org  jmeadows@gdc-uk.org	0121752 0103  0207167 6284
GDC	Freedom of Information	Luke Whiting	FOIRequests@gdc-uk.org	0207167 6309


### 10.3. Managerial Responsibility


Those who have managerial oversight or responsibility of the Data sharing under this Agreement

Organisation	Job Title	Name	Email	Phone
DBS	SIRO	Paul Whiting	paul.whiting2@dbs.gov.uk	0151 6761068
GDC	SIRO /Executive Director, Legal and Governance	Lisa-Marie Williams	lmariewilliams@gdc-uk.org	0207 1676 266



**11. Signatories**

SIGNED for and on behalf of Disclosure and Barring Service	Print Name:	Elaine Carlyle
	Position in organisation	Acting SIRO on behalf of Paul Whiting, CEO & Chief Financial Officer
	Date:	10.9.19

SIGNED for and on behalf of General Dental Council	Print Name:	LISA MARIE WILLIAMS
	Position in organisation	Executive Director, Legal and Governance
	Date:	04/09/2019

**12. Remarks**

Please use the space below for any remarks