



Disclosure &  
Barring Service

**Data Sharing Agreement**  
between:

Disclosure and Barring Service and  
General Pharmaceutical Council

**Table of Contents**

List of Acronyms ..... 3  
Document Control..... 4  
Form of Agreement..... 5  
Between..... 5  
1. Introduction ..... 6  
2. Purpose of the Agreement ..... 7  
3. Governance, monitoring, amendment and termination of this agreement.... 8  
4. Acknowledgements ..... 8  
5. Appendix 1: GDPR Principles ..... 9  
6. Appendix 2: Data Sharing Arrangements ..... 10  
7. Retention and Destruction..... 14  
8. The Data Security and Assurance Procedure ..... 15  
9. Responsibilities and commitments of both parties to this agreement..... 17  
10. Relationship Management ..... 19  
11. Signatories ..... 20  
12. Remarks..... 21

## List of Acronyms

CRB	Criminal Records Bureau
DBS	Disclosure and Barring Service
DPA	Data Protection Act 2018
DSA	Data Sharing Agreement
GDPR	General Data Protection Regulation
GPhC	General Pharmaceutical Council
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
20/06/2018	Initial draft	Donna Sheehan	0.1
06/08/2018	Amendments following 1 <sup>st</sup> Internal Review	Donna Sheehan	0.2
20/03/2019	Amendments following 1 <sup>st</sup> External Review	Donna Sheehan	0.3
24/04/2019	Amendments following 2 <sup>nd</sup> Internal Review	Donna Sheehan	0.4
28/08/2019	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	0.3
Catherine Nicholas	Legal Representative	0.3
Clare Burrows	Legal Representative	0.3
Michelle Anderson	Information Governance & Security Manager	0.3
David McLaren	Strategy & Policy	0.3
Andrea Walker	Associate Director	0.3
Mike Lowe	Head of Assurance	0.3
Stuart Mason	Assurance Manager	0.3
Helen Parks	DSA Lead	0.3
Donna Sheehan	DSA Officer	0.3
Barbara Moore	Team Leader	0.3
Katherine Bunting	Policy	0.3
Carole Gorman	GPhC Representative	0.4

### 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 28 August 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 Pharmaceutical Council (GPhC) whose address is  
25 Canada Square, London, E14 5LQ

## 1. Introduction

- 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 Lists)
- 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 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.
- 1.5.** The GPhC is the regulator for pharmacists, pharmacy technicians and pharmacy premises in England, Scotland and Wales. The overarching objective of the GPhC, set out in the Pharmacy Order 2010 is the protection of the public. This involves the following objectives:
  - to protect, promote and maintain the health, safety and wellbeing of the public;
  - to promote and maintain public confidence in the professions regulated by the GPhC;
  - to promote and maintain proper professional standards and conduct for members of those professions; and
  - to promote and maintain proper standards in relation to the carrying on of retail pharmacy businesses at registered pharmacies.

In addition, the GPhC has enforcement powers and duties under the Poisons Act 1972, the Medicines Act 1968 and the Veterinary Medicines Regulations. These enforcement duties/powers mainly relate to the sale and supply of medicines from registered pharmacies.

## 2. Purpose of the Agreement

- 2.1. This document is intended to act as an Agreement between the DBS and GPhC. 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 2018, 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.
- 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>	<b>Data Sharing Arrangements:</b> <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. 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 the DBS Senior Information Risk Owner (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 DBS 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 non compliance 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.

### 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 the GPhC from DBS or by using DBS systems or by any other means is subject to the [HMG Security Policy Framework](#) and GPhC agree that it will be processed in accordance with similar security controls for example ISO27001. 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.



## V 1.0 Data Sharing Agreement Template

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

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

Notwithstanding section 1.3; information will also be shared for the purposes listed in 6.1.1 below that helps employers make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups, including children.

### 6.1.2. The purposes include the following:

- a) In the interests of safeguarding vulnerable groups including children
- b) In the interests of public safety in healthcare, specifically pharmacy

### 6.1.3. The benefits of the data sharing:

- a) it assists DBS to fulfil its 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) promotes consultation on matters of safeguarding to improve both parties' performance in meeting their respective statutory duties and corporate objectives.
- d) promotes co-operation between the parties at an operational level and in the conduct of their respective statutory duties
- e) it will enable the GPhC to carry out its statutory function to protect the public and appropriately assess the fitness to practise of registered pharmacy professionals.

### 6.1.4. 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 may be shared and is determined on a case by case basis is information relating to:**

**From DBS to GPhC**

- Barred List status of an individual
- Data relating to individuals who are subject of a barring referral made by an employer or professional body on request.
- Copies of the relevant documents relating to the consideration bundle
- In cases where the DBS decides not to bar; if further information regarding the decision process 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 GPhC to DBS**

- Information received by the GPhC that constitutes the whole, or part, of a fitness to practise concern raised against a pharmacy professional, pharmacy owner or others involved in regulated activities
- Information gathered as a result of a fitness to practise investigation
- Information contained within a Fitness to Practise Consideration bundle
- Outcome decision from Fitness to Practise cases
- Information relating to an individual's status on GPhC Register
- DBS Referral form from GPhC including personal data and allegation information

**6.2.2 The data fields of the information to be shared include, where known and necessary:**

**From DBS to GPhC**

- Title
- Full Name
- Alias Name(s)
- Registration Number

**From GPhC to DBS**

- Title
- Full Name(s)
- Alias Name(s)

## V 1.0 Data Sharing Agreement Template

- Register Status
- Address(es)
- Date of Birth
- Alias Date of Birth
- NINO
- Nationality
- Gender
- Qualifications
- Position held
- Education and Training
- Barred List Status
- 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

#### From DBS to GPhC

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

#### From GPhC to DBS

- Information from GPhC secure server
- Paper Case Consideration Bundles
- Employer Referral Information
- Referral Information from another professional body, regulatory authority, public sector organisation or police and may include information from overseas organisations.

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

6.3.1 Both parties involved agree that they 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

## V 1.0 Data Sharing Agreement Template

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. for DBS:

- **Provision of Barring Information**  
Section 43: SVGA
- **Provision of information for 'fitness to practise' cases**  
Article 49: The Pharmacy Order 2010
- DBS acknowledge that there is the potential that the sharing of the information could constitute an interference with Article 8 of the Human Rights Act, right to respect for private and family life, but that any interference is held to be justifiable in all of the circumstances as the sharing of the information is deemed to be justified, necessary and proportionate. The sharing is undertaken in order to secure the protection of children and vulnerable adults.

### 6.3.5 GPhC:

- **Power to Refer**  
Section 41: SVGA
- **Duty to provide information on request**  
Section 42: SVGA
- **Disclosure of fitness to practise matters in the public interest**  
Section 50: The Pharmacy Order 2010
- 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 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

## V 1.0 Data Sharing Agreement Template

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

### 6.4.2. Between Organisations

- a) Where DBS data will be shared to support maintenance of the Register of Pharmacists and Pharmacy Technicians who are able to work or volunteer in regulated activity, GPhC will make the data sharing request in writing.
- 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 GPhC's 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) The GPhC will protect and store information provided by the DBS within a secure server.
- g) The method of Data Transfer between the two organisations will be via secure postal mail. Information will be double bagged, and DBS will also use email e.g. [dbsdispatch@dbs.gov.uk](mailto:dbsdispatch@dbs.gov.uk)
- h) The GPhC will make referrals following its own DBS referral policy.
- i) Referrals may be made using the DBS online referral tool or by secure postal mail
- j) GPhC's Referral Officer will have access to DBS data to carry out the activities agreed in this agreement. The Referral Officer will decide whether it is necessary and appropriate to disseminate information to select individuals which could include members of the Professionals Regulation Teams, statutory committees making decisions about a professional's fitness to practise or registrants, on a need to know basis.
- k) Both parties will process and handle the data in compliance with the GDPR/DPA 2018 and in line with the DBS Data Security and Assurance procedure (see section 8 below for more details).
- l) Neither party will process or otherwise transfer any Personal Data outside the European Economic Area without the other's consent.

## 7. Retention and Destruction

## V 1.0 Data Sharing Agreement Template

- 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 moratorium by Home Office information will be securely destroyed as soon as is practicable.
- 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. Both parties acknowledge 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. Both parties also acknowledge the requirement to maintain the confidentiality of data provided to it by the other party.
- 8.2. Both parties shall be responsible for the security of their own 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 as the minimum level required for security management;
  - Is commensurate with the threats to both parties' system.
- 8.3. Notwithstanding the above, both parties 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 respective controller, 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, both parties agree to:

## V 1.0 Data Sharing Agreement Template

- a) Ensure that there are adequate protective security measures in place to ensure the safeguarding of the storage, transmission or processing of data;
  - b) Limit access to the data to those persons required to carry out functions under this written Agreement save for where onward transmission is consistent with statutory or common law powers, in which case the other parties prior agreement 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 a breach of paragraph 8.5(d) occurring, both parties shall inform the respective controller immediately (using contacts listed on section 10 of this document) and within 24 hrs of becoming aware of any data breach. The controller will then follow its formal incident management process.
- 8.7. Both parties 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. Both parties will ensure that all of its staff including contractors with access to the other party's data:
- a) have undergone background verification 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. Both parties will ensure that there is auditable evidence that such safeguards are being applied.
- 8.10. Both parties 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 to the data processing change including in those circumstances listed below, both parties 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;



## V 1.0 Data Sharing Agreement Template

- d) If it becomes aware of any attempt to affect such compromise in respect of any data supplied by the other party.
- 8.12. Both parties will take appropriate legal action, in the event of misuse, unauthorised alteration, deletion of or access to or dissemination of data by staff including contractors or any third party.
- 8.13. Both parties will ensure that there are adequate protective security measures in place to ensure the safeguarding of the storage, transmission or processing of data provided to it under this Agreement and that any such measures have been assessed and agreed as appropriate.
- 8.14. Both parties will inform each other immediately and subsequently delete any information received from it which is not required for the data sharing and only retain the required data for as long as is necessary.
- 8.15. Both parties 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. Both parties will ensure that:
- a) its system is assessed for information risk and provide adequate controls for processing the other's 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 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 onsite or remote auditing or 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 GPhC 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.

## V 1.0 Data Sharing Agreement Template

- f) DBS to provide the information to GPhC 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.

### GPhC

- a) GPhC 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 onsite or remote auditing or the use of questionnaires.
- b) GPhC 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) GPhC to ensure that data is transferred to the DBS securely in accordance of its classification.
- e) GPhC to ensure staff handle 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) GPhC 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 GPhC will be undertaken by:

Organisation	Job Title	Name	Email	Phone
DBS	[IAO]	Karl Gergely	gergely.karl@dbs.gov.uk	01325953538
GPhC	Head of Service	Alicia Marsh	alicia.marsh@pharmacyregulation.org	02037137877

### 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	01516761559
DBS	Information Governance and security Manager	Michelle Anderson	michelle.anderson3@dbs.gov.uk	01325953602
DBS	Relationship Management	Stuart Mason	stuart.mason@dbs.gov.uk	01325953839
DBS	Freedom of Information	Karl Gergely	gergely.karl@dbs.gov.uk	01325953538
DBS	Operational Contact	Barbara Moore	barbara.moore@dbs.gov.uk	01325953533
GPhC	Data Protection Officer	Carole Gorman	Carole.gorman@pharmacyregulation.org	02037137827
GPhC	Relationship Management	Sharon Charles	sharon.charles@pharmacyregulation.org	02037137844
GPhC	Operational contact	Anna Sutton	anna.sutton@pharmacyregulation.org	02037137829
GPhC	Freedom of Information	Carole Gorman	foi@pharmacyregulation.org	02037137827


### 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@dbb.gov.uk	01516761068
GPhC	Director of Insight, Intelligence and Inspection	Claire Bryce-Smith	Claire.bryce-smith@pharmacyregulation.org	02037138000

## 11. Signatories

<p>SIGNED</p>  <p>for and on behalf of Disclosure and Barring Service</p>	Print Name:	Paul Whiting
	Position in organisation	Chief Financial Officer (SIRO)
	Date:	3.10.19

<p>SIGNED</p>  <p>for and on behalf of <b>GPhC</b></p>	Print Name:	Claire Bryce-Smith
	Position in organisation	Director of Insight, Intelligence and Inspection
	Date:	2 <sup>nd</sup> October 2019

## 12. Remarks

Please use the space below for any remarks