



**Disclosure &
Barring Service**

Data Sharing Agreement
between:

**Disclosure and Barring Service and
Care Quality Commission**

Table of Contents

List of Acronyms.....	3
Document Control	4
Form of Agreement	5
Between	5
1. Introduction.....	5
2. Purpose of the Agreement.....	6
3. Governance, monitoring, amendment and termination of this agreement	7
4. Acknowledgements	8
5. Appendix 1: Data Protection/GDPR Principles	9
6. Appendix 2: Data Sharing Arrangements	9
7. Retention and Destruction.....	16
8. The Data Security and Assurance Procedure.....	16
9. Responsibilities and commitments of both parties to this agreement.....	19
10. Relationship Management	20
11. Signatories.....	22
12. Remarks	22

List of Acronyms

CQC	Care Quality Commission
CRB	Criminal Records Bureau
DBS	Disclosure and Barring Service
DPA	Data Protection Act 2018
DSA	Data Sharing Agreement
GDPR	General Data Protection Regulation (EU) 2016/679
HSCA	Health and Social Care Act 2008
IAO	Information Asset Owner
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

V 1.0 Data Sharing Agreement Template

Document Control

REVISION HISTORY

Date	Comments	Author	Version
05/04/2018	Initial Draft	Donna Sheehan & Lisa Grimstead	0.1
20/04/2018	Amendments made following 1 st review	Helen Parks	0.2
01/05/2018	Amendments following first internal Review	Lisa Grimstead	0.3
03/05/2018	Amendments following quality check	Helen Parks	0.4
21/05/2018	Amendments made following external review	Donna Sheehan	0.5
05/06/2018	Amendments made following 2 nd internal review	Lisa Grimstead & Donna Sheehan	0.6
13/06/2018	Further amendmets made following Legal surgery and DPA 2018 referenced	Donna Sheehan & Lisa Grimstead	0.7
15/06/2018	Amendments following QC	Helen Parks	0.8
27/09/2018	Amendments made following 2 nd external review	Donna Sheehan & Helen Parks	0.9
23/10/2018	Baselined to V1.0	Helen Parks	1.0

REVIEWERS

THIS DOCUMENT HAS BEEN ISSUED TO THE FOLLOWING FOR REVIEW:

Name	Job role	Version
Karl Gergely	Information Asset Owner	0.9
Catherine Nicholas	Legal Representative	0.9
Clare Burrows	Legal Representative	0.9
Michelle Anderson	Information Governance and Security Manager	0.9
David McLaren	Strategy & Policy	0.9
Andrea Walker	Associate Director	0.9
Phil Serrecchia	Head of Quality and Excellence HUB	0.9
Stuart Mason	Assurance Manager	0.9
Helen Parks	DSA Lead	0.9
Donna Sheehan	DSA Officer	0.9
Barbara Moore	Team Leader	0.9
Karen Culshaw	CQC Regulatory Policy Manager	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 16th October 2018

Between

Disclosure and Barring Service (DBS) whose address is
Stephenson House, Alderman Best Way, Morton Palms Business Park,
Darlington, County Durham, DL1 4WB

And

Care Quality Commission (CQC) whose address is
151 Buckingham Palace Road, London, SW1W 9SZ;

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 List's)
- 1.3. The CQC is a Non-Departmental Public Body (NDPB) sponsored by the Department of Health and Social Care. It is established under the Health and Social Care Act 2008 (HSCA 2008) and it carries out functions previously undertaken by the Commission for Social Care Inspection, Healthcare Commission and the Mental Health Act Commission. The CQC monitor,

V 1.0 Data Sharing Agreement Template

inspect and regulate health and social care services and publish findings, including ratings to help people choose care.

1.4. It is responsible for:

- 1.4.1. Registering health and social care providers under the Health and Social Care Act 2008.
- 1.4.2. Monitoring, inspection and rating of health and social care services.
- 1.4.3. Taking action to protect people who use services.
- 1.4.4. Giving an independent voice and publishing our views on major quality issues in health and social care.

1.5. Information can be shared between both parties 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 Health and Social Care Act 2008, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

1.6. Both parties operate 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.

2. Purpose of the Agreement

2.1. This document is intended to act as an Agreement between the CQC 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: the GDPR, the 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 parts are inseparable and shall form the entire Agreement.

2.6. Part 2 contains the following Appendices.

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

3. Governance, monitoring, amendment and termination of this Agreement

3.1. The governance and monitoring of this Agreement will be undertaken by both parties. Formal reviews will be undertaken at least annually or at a shorter duration depending on the duration of the Agreement and will be initiated by DBS.

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 Senior Information Risk Owner (SIRO) of both parties.

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;

- 3.3.4. In the event of non compliance with the terms set out in this Agreement or a significant security breach by either party. A security breach or serious breach is failure to comply with any requirement of either parties' information security policies and processes.

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 CQC from DBS or by using DBS systems or by any other means is subject to the [HMG Security Policy Framework](#) and CQC 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.
- 4.1.3. DBS and CQC 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 2018.

Both parties are Data Controller in their own right and therefore accepts that this Agreement treat them as such. The receiving organisation will become the data controller upon receipt of information from the sending organisation.

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

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.

6.1.1. The purposes include the following:

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

V 1.0 Data Sharing Agreement Template

- b) In the interests of allowing both parties to fulfil their statutory obligations

6.1.2. The benefits of the data sharing

- a) It assists the 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) It assists the CQC to fulfil its obligations under the HSCA2008
- d) Information provided to CQC will assist in the registration decision making process and inspection decisions
- e) It promotes co-operation between the parties at an operational level and in the conduct of their respective statutory duties
- f) It promotes consultation on matters of safeguarding to improve both parties' performance in meeting their respective statutory duties and corporate objectives

6.1.3 The desired outcome for this data sharing is to:

- a) Improve operational 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 and CQC 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 CQC

- Barred List status of an individual
- Data relating to individuals who are subject of a barring referral made by an employer or professional

From CQC to DBS

- Information about allegations held within a referral relating to Registered Managers, Proprietors and Directors of Care providers
- A copy of any inspection

V 1.0 Data Sharing Agreement Template

body on request

- On request, if further information is required, the DBS will provide a list of documents held by the DBS in relation to the case. The DBS will then provide such documents from the list as requested by CQC and relevant to the matter
- In cases where the DBS decides not to 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 the information from a Disclosure Information Print

documentation

- A copy of the investigation outcome letter
- A copy of any concerns referred to CQC relating to individuals by members of the public, staff at care services and other health and care professionals.

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

From DBS to CQC

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

From CQC to DBS*

- Title
- Full Name(s)
- Alias Name(s)
- Address(es)
- Date of Birth
- Registration Number
- Alias Date of Birth
- NINO
- Nationality
- Gender
- Qualifications
- Position Held
- Education and Training
- Additional data required within the DBS referral form

*CQC would only hold this level of personal data for a registered manager or nominated individual.

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

From DBS to CQC

- Siebel
- Paper Case Files
- Employer Referral Information
- Disclosure Information Print
- CQC Website

From CQC to DBS

- Paper Case consideration Bundles
- Inspection reports
- Employer Referral Information
- CRM System

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. Where one party has found that incorrect information has been shared with another, reasonable steps shall be taken to inform the other party of any inaccuracies and corrections made to information.

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 47 (1) - (4): SVGA
- Section 50: SVGA

DBS acknowledge that there is the potential that the sharing of 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 circumstances as the sharing of information is deemed to be justified, necessary and proportionate. The sharing is undertaken in order to secure the protection of children and vulnerable adults.

- 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.

6.3.5 For CQC:

- **Power to Refer**
Section 45: SVGA
- **Duty to Provide Information on Request**
Section 46: SVGA

V 1.0 Data Sharing Agreement Template

CQC acknowledges that there is the potential that the sharing of 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 circumstances as the sharing of information is deemed to be justified, necessary and proportionate. Any sharing is undertaken in line with CQC's own information sharing guidance and the CQC Code of Practice on Confidential Personal Information (CPI).

- Section 77 of the Health and Social Care Act 2008 provides a defence to the offence of disclosure of CPI (section 76 HSCA 2008) where disclosure of information is required by law, necessary for protecting the welfare of any individual or necessary for the facilitating the statutory functions of another organisation.
- Section 79 of the Health and Social Care Act 2008 permits disclosure of any information held by CQC (including CPI and personal data) where disclosure of information is required by law, necessary for protecting the welfare of any individual or necessary for the facilitating the statutory functions of another organisation.

6.4 Procedure for the Data Sharing

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

6.4.2 From DBS to CQC

- a) Where DBS data will be shared to support CQC in its role of inspection, registration and monitoring of establishments, CQC 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 the CQC.
- 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 as and when information is requested.
- f) The CQC will protect and store information provided by the DBS by storing data in secure computer files with restricted access ie. Only staff with a business need will access the information. All paper files are stored securely within the relevant department.

- g) The method of Data Transfer between the parties will be via secure postal mail. Information will be double bagged and DBS also use a secure email address e.g. dbsdspatch@dbs.gov.uk
- h) The CQC's Inspectors, Counter Signatories, and Lead Counter Signatory will have access to DBS data to carry out the activities agreed in this agreement.
- i) The CQC will process and handle the data in compliance with the GDPR/DPA and in line with CQC's own internal information security processes.
- j) Not Process or otherwise transfer any Personal Data outside the European Economic Area without DBS consent.

6.4.3 From CQC to DBS

- a) Where CQC data will be shared to support DBS in its role of assessing people for DBS barred lists, DBS will make the request in writing, and where appropriate state the appropriate legislation under which the request is made.
- b) CQC inspection teams will consider the request against the information sharing guidance, and whether there is a legal basis for disclosure under section 77/79 of the Health and Social Care Act 2008.
- c) Where an inspection team cannot determine a legal basis for sharing they will seek advice from the Information Access Team.
- d) Once the legal basis has been determined, the inspection team shall document the reasons for sharing within the CQC CRM system.
- e) The volumes of data shared may vary and will be responded to on an ad hoc basis as and when information is requested.
- f) The DBS will protect and store information provided by the CQC securely and in line with the GDPR/DPA. Access to systems is controlled by role based access controls (RBAC). Only authorised staff with a legitimate business interest will have access to the data.
- g) The method of Data Transfer between the two organisations will be via secure postal mail. Information will be double bagged and DBS also use a secure email address e.g. dbsdspatch@dbs.gov.uk
- h) The DBS employees will have access to CQC data to carry out the activities agreed in this agreement.
- i) The 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).
Not Process or otherwise transfer any Personal Data outside the European Economic Area without DBS consent.

7 Retention and Destruction

- 7.1. Where both Parties are Data Controllers, they 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 both parties 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.

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 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

V 1.0 Data Sharing Agreement Template

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 the from the other party, both parties 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;
- 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 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 parties 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:

V 1.0 Data Sharing Agreement Template

- 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. 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) it's 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 CQC 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 CQC 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.

CQC

- a) CQC 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) CQC 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) CQC to ensure that data is transferred to the DBS securely in accordance of its classification.
- e) CQC to ensure staff handle data in line with the approved secure transfer method agreed by both parties and within the data security classification of the data and ensure retention policy and data destruction policy is adhered to.
- f) CQC 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 CQC will be undertaken by:

Organisation	Job Title	Name	Email	Phone
DBS	[IAO]	Karl Gergely	gergely.karl@dbb.gov.uk	01325 953538
CQC	[IAO] / Head of Service	James Nolan	james.nolan@cqc.org.uk	07471 020634

10.2. Business Contacts

The Business contacts of this Agreement are:

Organisation	Role	Name	Email	Phone
DBS	Data Protection Officer	Elaine Carlyle	elaine.carlyle@dbb.gov.uk	0151 6761559
DBS	Information Governance & Security Manager	Michelle Anderson	michelle.anderson3@dbb.gov.uk	01325 953602
DBS	Relationship Management	Stuart Mason	stuart.mason@dbb.gov.uk	01325 953839
DBS	Freedom of Information	Paul Rogers	paul.rogers2@dbb.gov.uk	01325 953793
DBS	Operational Contact	Barbara Moore	barbara.moore@dbb.gov.uk	01325 953533
CQC	Data Protection Officer	Nimali de Silva	nimali.desilva@cqc.org.uk	07384 437335

V 1.0 Data Sharing Agreement Template

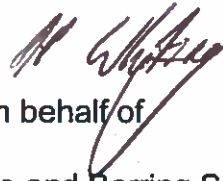
CQC	Information Rights Manager	Simon Richards on	simon.richardson@cqc.org.uk	0191 2333599
CQC	Information Security Manager	Derek Wilkinson	derek.wilkinson@cqc.org.uk	07785 447103
CQC	Relationship Manager	Karen Culshaw	karen.culshaw@cqc.org.uk	07789 876253
CQC	Freedom of Information		information.access@cqc.org.uk	
CQC	Operational Contact, National Advisor Safeguarding	Janice Waters	janice.waters@cqc.org.uk	07467 001433


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 Name]	Paul Whiting	paul.whiting2@db.gov.uk	0151 6761068
CQC	Executive Director of Strategy & Intelligence/ SIRO	Malte Gerhold	malte.gerhold@cqc.org.uk	0207 4489060

11. Signatories

SIGNED  for and on behalf of Disclosure and Barring Service	Print Name:	Paul Whiting
	Position in organisation	Deputy Chief Executive & Chief Financial Officer (SIRO)
	Date:	16 th November 2018

SIGNED for and on behalf of the CQC	Print Name:	Peter Sinden
	Position in organisation	Chief Digital Officer
	Date:	15/11/2018

12. Remarks

Please use the space below for any remarks