

DATA SHARING AGREEMENT

OFFICE OF THE PUBLIC GUARDIAN (SCOTLAND)

And

THE MENTAL WELFARE COMMISSION FOR SCOTLAND

June 2022

Version v.1

Contents

Introduction.....	3
1. Parties ('the Parties'/'the Party') to the Data Sharing Agreement.....	3
2. Business and legislative drivers for sharing data.....	3
3. Purpose and description of the information to be shared	4
4. Approach to data sharing.....	6
5. Communications and single points of contact.....	11
6. Review and Termination of the Data Sharing Agreement	11
7. Resolution of disputes with Data Subjects or the Information Commission's Office 11	
8. Language.....	11
9. Escalation Procedure	12
10. Term and Termination	12
11. Variation	12
12. Legal Status of this Data Sharing Agreement.....	12
13. Governing Law and Jurisdiction.....	12
14. Signatures	13

Introduction

1. This agreement covers the sharing of personal data by **The Office of the Public Guardian (Scotland)** with **The Mental Welfare Commission for Scotland** and vice versa. Both Parties have functions prescribed by law and written in statute which are likely to provide a lawful basis for sharing personal, sensitive data where sharing is necessary for the exercise of those functions, proportionate, and carried out in accordance with the rights of the data subjects.

2. This agreement takes into account and should be construed and applied in accordance with relevant Data Protection, Human Rights and Freedom of Information legislation. The organisation to whom the data is transferred will become the data controller of that information for the purposes for which it is transferred. Nothing in this agreement means that either Party is processing data on behalf of the other.

3. This agreement does not generally apply to the sharing of non-personal data but there are situations where sharing non-personal data may increase a risk of identification and this is also dealt with in this agreement.

1. Parties ('the Parties'/'the Party') to the Data Sharing Agreement

The Mental Welfare Commission for Scotland (the Commission/MWC) is an independent organisation set up by Parliament with a range of duties prescribed under mental health and incapacity law, namely the Mental Health (Care and Treatment) (Scotland) Act 2003 and the Adults with Incapacity (Scotland) Act 2000 (the AWI Act). The Commission is accountable to Scottish Ministers for its statutory duties.

The Office of the Public Guardian (Scotland) (the OPG) is part of Scottish Courts and Tribunals Service (the "SCTS"), and was established in April 2001 following the passing of the Adults with Incapacity (Scotland) Act.

The Commission and the OPG are considered independent controllers of the data collected, as both parties separately determine the means and purpose of processing personal data as part of the functions defined in this agreement.

2. Business and legislative drivers for sharing data.

2.1 The Commission has responsibilities to protect and promote the rights of adults who by reason of a mental health condition are regarded as adults with incapacity under the AWI Act. It works to safeguard the rights and welfare of individuals with a mental illness, learning disability, dementia or related condition.

It monitors the use of the welfare provision of the AWI Act and it has wider role in promoting best practice in the use of mental health law; ensuring that the care and treatment of a person with a mental health condition is in line with the principles of mental health law.

The Commission also monitors aspects of Part 5 of the AWI Act relating to consent to medical treatment.

2.2 The OPG has a general function to maintain a public register of all orders made under the AWI Act, including Powers of Attorney, Guardianship and Intervention Orders granted and authorisations granted under the Access to Funds scheme.

Functions also include:

- (a) Registering Powers of Attorney deeds that are to begin or continue in the event of incapacity.
- (b) Supervising those individuals who have been appointed to manage the financial and property affairs of adults who lack the capacity to do so for themselves.
- (c) Investigating circumstances, where the property or finances belonging to an incapable adult appear to be at risk.

2.3 The Parties recognise that both organisations have functions and duties prescribed by legislation which are likely to provide a lawful basis for sharing additional personal, sensitive data in accordance with the rights of the data subjects.

2.4 The OPG and MWC also have a mutual responsibility, under the AWI Act, to consult on cases on matters relating to the exercise of functions under the AWI Act in which there is, or appears to be, a common interest.

3. Purpose and description of the information to be shared

3.1 MWC monitoring and safeguarding role.

For the Commission to perform its statutory duties it requires access to information about adults with incapacity, welfare powers of attorney, intervention orders and guardianship orders. This information is routinely collected and registered by the OPG. For some of this information, the OPG has a legal obligation to notify the Commission set out in the AWI Act (Part 2 and Part 6 AWI Act).

In addition to statutory notifications from the OPG, the Commission may receive information from other parties during the guardianship order process. Sometimes this

information is not sent on time to the Commission or it is incomplete. When this happens the Commission will request access to additional information held by the OPG.

In particular, the Commission will request from the OPG, guardianship order applications (section 57 AWI Act) when it has been unable to obtain it from elsewhere.

The Commission requires to have accurate information about granted guardianship orders and the circumstances of the adult with incapacity in order to monitor accurately the application of the AWI Act and produce monitoring reports. This information is also relevant for undertaking guardianship visits. The papers sent by the OPG under section 58 AWI Act (disposal of application), once the orders have been granted by the Court, are not always sufficient for the Commission to perform its duties in the event the Commission has not previously received application paperwork (s.57 AWI Act).

When the Commission is aware that relevant information in relation to diagnosis is missing from Commission records, it will request, after having attempted to get the information from the relevant source first, that the OPG provide any additional relevant information to the Commission.

3.2 MWC and OPG Investigations

For the purposes of any investigation mentioned in the AWI Act s.6 (2)(c) or (d) and s.9(1)(d) by the Commission, the OPG and the Commission shall provide each other with such information and assistance as may be necessary to facilitate the investigation.

3.3 Other matters of concern

The OPG will inform the MWC immediately of any deficiency in care and treatment and welfare issues which give rise to any concern which is within the contemplation of the OPG. Similarly, the MWC will inform OPG when it becomes aware of concerns about adults with incapacity at risk of financial abuse.

3.4 Categories of data

The information to be shared between both bodies includes personal data and special categories of data as defined by the GDPR Article 9 and section 3 (2) of the Data Protection Act 2018.

The following types of data may be held by the OPG and may be considered for release:

- title, full name, gender
- home address and contact details
- date of birth, national insurance number
- representatives, appointees and their contact details.
- details of care providers including data about any relevant health condition and diagnosis

4. Approach to data sharing

4.1 Data flows

The Commission uses NHS mail and this means that transactions of personal data between MWC and other high accredited secure emails, like gov.uk, are encrypted and acknowledged to be secure.

The OPG will send the statutory notifications to the MWC by secure email to mwc.support@nhs.scot.

Additional information could be requested when necessary for the purposes explained in section 3. The OPG will respond to any specific written request for information within the scope of this agreement promptly by sending the information by encrypted email to the requester (OPGdatashare@scotcourts.gov.uk)

Sensitive personal data shared with the Commission is stored on a secure server and is password protected. All Commission IT equipment, including laptops, is compliant to at least the minimum requirements contained within NHS Scotland's IT Security Standards. Double encryption of devices, including laptops, is standard. The Commission has the Cyber Essential accreditations and it is working towards obtaining the Cyber essential plus.

As part of the Commission's induction programme, all staff are made aware by the Information Manager of Data Protection principles and the importance of managing information risk. The Commission has IT and information policies, which are available on our intranet. Key policies, including our Information Risk Management Policy, form part of the employment contract and staff must indicate that they have understood and agree to abide by each of the policies.

The Commission's data breach policy has details of the actions required in the event of data loss, corruption or theft. This policy includes all the required reporting mechanisms, up to and including reporting to the Information Commissioner's Office.

Shared data will be reviewed by the relevant internal teams.

4.2 Data controllers' declaration

The Parties agree that they will be controllers with separate purposes and processes in relation to this data sharing agreement (DSA) and that each is therefore responsible for complying with the Data Protection Act 2018 in relation to any personal data that is processed pursuant to this agreement. Where the OPG shares data with the Commission, the OPG will remain the controller of that data until the data is received by the Commission. Where the Commission shares data with the OPG, the Commission will remain the controller of that data until it is received by the OPG.

4.3 Lawful and Fair

Each party shall ensure that it processes the Personal data fairly and lawfully in accordance with Article 5 (1) (a) of the UK GDPR.

Without detriment of any other legal basis that may be applicable (e.g. criminal investigation, etc.) the following is the core legal basis for each of the parties to process the data in this agreement:

Processing	Legal basis	Party
MWC monitoring and safeguarding role (Part 2 and Part 6 AWI Act)	UK GDPR Article 6.1 (c). Processing is necessary for the compliance of a legal obligation.	OPG
MWC monitoring and safeguarding role; MWC and OPG Investigations; Other matters of concern.	UK GDPR Article 6.1 (e). Processing is necessary for the performance of a public task carried out in the public interest.	MWC/OPG

<p>MWC monitoring and safeguarding role; MWC an OPG Investigations; Other matters of concern.</p>	<p>UK GDPR Article 9.2 (g) Substantial public interest, on the basis of Domestic law. This requirement is met as outlined under The DPA Section 8 and Schedule 1, Part 2 Paragraph 6 for the purpose of exercising a function conferred on a person by enactment or rule of law (Adults with Incapacity (Scotland) Act 2000).</p>	<p>MWC/OPG</p>
<p>Archiving of records in line with requirements under Public Records Scotland Act, 2011. Undertaking research or creating statistical outputs in line with legislative or business requirements such as annual reports and accounts as outlined in respective privacy notices.</p>	<p>UK GDPR Article 9.2.j Archiving, research and statistical purpose</p>	<p>MWC/OPG</p>
<p>MWC monitoring and safeguarding role. Equality of opportunity and treatment.</p>	<p>UK GDPR Article 9.2 (g) Substantial public interest on the basis of Domestic law. This requirement is met as outlined under The DPA Section 8 and Schedule 1, Part 2 Paragraph 8: Identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in</p>	<p>MWC/OPG</p>

	relation to that category with a view to enabling such equality to be promoted or maintained.	
--	---	--

4.4 Transparent processing.

During the Term of this DSA, each Party will be responsible for updating its privacy notice to include the sharing of personal data set out in this agreement.

The Commission’s privacy statement is available on its website at (<https://www.mwcscot.org.uk/>)

The OPG privacy statement is available [Data Protection \(scotcourts.gov.uk\)](https://www.scotcourts.gov.uk/data-protection)

4.5 Individual Rights Requests

Individuals whose personal data is being processed under this DSA have the right to make individual rights requests to the relevant organisation(s) party to this DSA and to make a request for access to personal data and to consider rectifying data or erasing if they advise that the data held by either or both Parties is inaccurate. The Parties will have primary responsibility for responding to individual rights requests as it relates to their respective organisation.

4.6 Accuracy and Limitation

The organisation sharing data will seek to ensure that it is up-to-date and accurate before it is shared. If either Party becomes aware of any concerns about the accuracy or quality of the data after it has been shared they should contact the other organisation as soon as possible.

Each party shall ensure that the Personal data is:

- (i) Adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data is processed under this DSA; and
- (ii) Accurate and, where necessary, up to date; having taken every reasonable step to ensure that any inaccurate personal data (having regard to the purposes for which the personal data is processed under this DSA) has been erased or rectified.

Information provided to the Commission should only be used for the purposes set out in this DSA.

4.7 Data Retention and Deletion

The Parties shall not retain or process personal data for longer than is necessary to carry out the agreed purposes as set out in clause 3 of this DSA. The Parties shall establish and adhere to appropriate archiving arrangements as set out in the Parties' respective records management plans.

4.8 Security and Training

The Parties undertake to have in place throughout the Term (as set out in clause 10 of this DSA) appropriate technical and organisational security measures to:

- (i) prevent:
 - unauthorised or unlawful processing of the personal data ; and
 - the accidental loss or destruction of, or damage to, the personal data

- (ii) ensure a level of security appropriate to:
 - the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
 - the nature of the personal data to be protected.

It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and process the personal data in accordance with the technical and organisational security measures set out in **s.2 article 32** of the UK GDPR together with any other applicable national data protection laws and guidance.

4.9 Personal data breaches and reporting procedures

A personal data breach is defined in the UK GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transfer between parties, stored or otherwise processed in accordance with this agreement.

The parties shall inform the other party if appropriate of any Personal Data Breach irrespective of whether there is a requirement to notify the Information Commissioner or Data Subject(s) and each Party shall comply with their obligations under **Article 33** of the UK GDPR to report a Personal Data Breach to the Information Commissioner and (where applicable) Data Subjects.

The parties agree to provide reasonable assistance, as is necessary, to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

4.10 International transfer of personal data.

Personal data shared in line with this agreement will be not be transferred outside the UK.

5. Communications and single points of contact

Each Party will appoint a single point of contact (**SPoC**) who will work together to reach an agreement with regards to any issues arising from data processing as it relates to this DSA and to actively improve the effectiveness of the data sharing initiative. The points of contact for each of the parties are:

- a) The Chief Executive of the Mental Welfare Commission
- b) The Public Guardian, Office of the Public Guardian Scotland

6. Review and Termination of the Data Sharing Agreement

Parties shall review the effectiveness of this data processing initiative every 3 years giving consideration to the aims and purposes listed in **Clause 2 and 3**. The Parties shall continue, amend or terminate the DSA depending on the outcome of this review.

The review of the effectiveness of the data processing initiative will involve assessing whether the purposes for which the personal data is being processed and the category of personal remain relevant and accurate.

Each Party reserves its rights to inspect the other party's arrangements for the processing of Personal data within the terms of this agreement with respect to the legal framework governing data quality, retention, and Data Subjects' rights, and to terminate the DSA where it considers that the other party is not processing the Personal data in accordance with this DSA.

7. Resolution of disputes with Data Subjects or the Information Commission's Office

In the event of a dispute or claim brought by a Data Subject or the Information Commissioner's Office in relation to information shared under this agreement, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

8. Language

If this DSA is translated into any other language, the original English language version shall prevail.

Any notice given under or in connection with this DSA shall be in English. All other documents provided under or in connection with this DSA shall be in English.

9. Escalation Procedure

If either Party receives any formal inquiry, complaint, claim or threat of action from a third party (including, but not limited to, requests for information made under the **Freedom of Information (Scotland) Act 2002**) in relation to this DSA, the matter shall be promptly referred to the SPoC of each Party (or its nominated representatives). No action shall be taken in response to any such inquiry, complaint, claim or action, to the extent that such response would adversely affect this DSA without the prior approval of the other Party.

10. Term and Termination

This Data Sharing Agreement shall commence on 6 June 2022 and shall continue unless terminated earlier in accordance with **Clause 6**

A Party may terminate this Data Sharing Agreement by giving the other Party at least three months' notice in writing at any time.

11. Variation

This Data Sharing Agreement may only be varied by written agreement of the Parties.

12. Legal Status of this Data Sharing Agreement

This Data Sharing Agreement is not intended to be legally binding, and no legal obligations or legal rights shall arise between the Parties from this Data Sharing Agreement. The Parties enter into the Data Sharing Agreement intending to honour all their obligations. This Data Sharing Agreement is intended to comply with the UK GDPR Article 24 and/or the Data Protection Act 2018.

13. Governing Law and Jurisdiction

This Data Sharing Agreement shall be governed by and construed in accordance with Scots law.

14. Signatures

I hereby agree to the terms set out in the Data Sharing Agreement

For and on behalf of the Mental Welfare Commission



Name: Julie Paterson

Position: Chief Executive, Mental Welfare Commission

Date: 06/06/2022

For and on behalf of the Office of the Public Guardian (Scotland)



Name: Fiona Brown

Position: Public Guardians & Accountant of Court

Date: 06/06/2022