

Data Sharing Agreement

between

Sandwell Metropolitan Borough Council

and

Brushstrokes Community Project (part of Father Hudson's Care)

Date: _1st_/_October_/2020

Version	24 th September 2020
Amendments made by	
Review Date	September 2021

Introduction

This Agreement sets out the overarching data sharing protocol between Sandwell Metropolitan Borough Council (SMBC) and Brushstrokes Community Project (Father Hudson's Care)

The intent of this Agreement is to ensure that SMBC and Brushstrokes Community Project, in sharing information, comply with the statutory and legislative requirements relating to the disclosure of personal information including the General Data Protection Regulations (2016/279), the Data Protection Act 2018, the Human Rights Act 1988 and the common law duty of confidentiality.

By endorsing this Agreement, the parties signal their commitment to openness, transparency, security and confidentiality of personal information, sensitive information and business critical information. It will provide, appropriate governance and support assurance to the parties in fulfilling their duties as data controllers, ensuring the safe, lawful and secure sharing of personal data.

Scope

The conditions and requirements within this Agreement will apply to all employees, officers, agents, elected representatives, volunteers, management, contractors and sub-contractors working on behalf of the parties.

This Agreement will cover the following:

- Sharing between the Parties as Data Controller sharer (both Parties) to Data Controller recipient (both Parties).

WORD/PHRASE	DEFINITION
Controller	As defined in Article 4 of the GDPR.
Data	as defined within the GDPR and the DPA, including both Personal and Sensitive Data, and also any Data which is not defined by the DPA and which comprises any written information which is provided to or acquired by the Parties which is either (a) commercially sensitive, or (b) confidential, or (c) Special Categories of Personal Data and (d) 'information asset'
Data Protection Legislation	<p>The statutes, regulations, codes and guidance to include (bit limited to) the following:</p> <ul style="list-style-type: none"> i) The General Data Protection Regulation (Regulation (EU) 2016/679) (the 'GDPR'); ii) The Data Protection Act 2018 and any subsequent Data Protection legislation (the 'DPA'); iii) The EU Data Protection Directive 95/46; iv) The Regulation of Investigatory Powers Act 2000; v) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; vi) The Electronic Communications Data Protection Directive 2002/58/EC; vii) The Privacy and Electronic Communications (EC Directive) Regulations 2003; viii) All applicable laws, and regulations relating to the Processing of Data and privacy including (where applicable and without limitation) the guidance and codes of practice issued by the Information Commissioner under the GDPR, DPA and under any subsequent Data Protection legislation. <p>This will also include any statutes, regulations, codes and guidance which may come into force at a future date.</p>
Data Subject	The identifiable natural person to whom the Personal Data belongs
DPA	The current Data Protection Act 2018 and any subsequent Data Protection Legislation.
DPO	Data Protection Officer
Fair Processing Notice	Information provided to the individual either when collecting the information, or at the point of receipt of the information from a third party. This notice must comply with the requirements of Articles 12, 13 and 14 of the GDPR and any relevant Data Protection Legislation.

Filing System	Any structured set of Data which is accessible according to specific criteria, whether centralised, de-centralised or dispersed on a functional or geographic basis
GDPR	The General Data Protection Regulation (Regulation (EU) 2016/679)
ICO	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. The UK independent authority for regulating and monitoring activity under all relevant Data protection and information rights legislation.
In Writing	Any reference to 'in writing' or 'written' shall be construed to mean to trace or form or transcribe (characters, letters, words etc.) on paper and or in electronic formats, such as in letters, records or in email that captures information that falls under the processing conditions of this Protocol.
Information Asset Owner	A designated senior officer with ownership and responsibility for specific information assets (including paper based and electronic records and IT systems)
Joint Controllers	As provided in Article 26 of the GDPR
Party/Parties	SMBC and Brushstrokes Community Project
Personal Data/ Personal	As defined in Article 4 (1) of the GDPR
Personnel	All employees of the Processor, or its suppliers, contractors, sub-contractors, officers, agents, students on work experience and volunteers who are from time to time employed and/or engaged in connection with processing Data on behalf of the Data Controller or otherwise in relation to the performance of a contract.
Privacy Notice	This shall have the same meaning as Fair Processing Notice.
Processing / Processed / Process	The definition for Processing/Processed/Process within this Protocol shall have the same meaning as Processing within Article (4) (2) of the GDPR
Processor	As defined in Article 4 of the GDPR
Protocol	This document and all of its schedules and any variations to it. All Parties to the Protocol must agree any variations in writing.
Working Days	Any day that is not a Saturday, Sunday or public holiday in England.

1. Purpose for Sharing Information

- 1.1 Effectively sharing information will bring significant benefits in supporting vulnerable Sandwell residents in need of immigration, welfare benefits, housing and other advice, as well as a range of community-based support services provided by Brushstrokes Community Project. Brushstrokes is tasked by the Local Authority to support: asylum seekers, refugees, people with no recourse to public funds, newcomers in need of support to settle in Sandwell, residents in need of advice to formalise their immigration status (including EU Settled Status).
- 1.2 Information will be used to deliver services and enhance decision making on a case-by-case basis. Sharing data will enable services to be targeted and delivered effectively.
- 1.3 Information shared will be personal or sensitive or both and to achieve the following objectives:
- 1.3.1 To fulfill the Local Authority's obligations with regard to safeguarding and social protection;
- 1.3.2 To carry out consultation and continually improve public services;
- 1.3.3 To carry out statutory and regulatory functions relating to social care assessments involving vulnerable children and vulnerable adults, the prevention of homelessness by supporting people at risk of homelessness and safeguarding vulnerable people.
- 1.3.4 To meet legal requirements and comply with legal obligations;
- 1.3.5 To prevent or detect crime and fraud and to protect individuals from harm;
- 1.4 The above purposes are not exhaustive.

2. Personal Information to be Shared

Personal information to be shared under this agreement include:

- Name, title and address
- Gender, date of birth and age
- Ethnicity and country of origin
- Immigration status
- Email, mobile, telephone

3. Means of Information Transfer

Organisation	Secure e-mail address	Other methods
--------------	-----------------------	---------------

SMBC	Sandwell.gov.uk TLS 1.2 encryption	
Brushstrokes Community Project	Office 365 encryption (OME)	

4. Period of Agreement

The Agreement commences on _1st_/_October/_2020_ to be reviewed by _30th_/_September/_2021_

5. Legal basis for sharing information

5.1 Personal data should be shared fairly and lawfully. In order to achieve this, the parties must comply with at least one condition from Article 6 and, where special category (sensitive) information is included, at least one condition from Article 9 of the GDPR.

Article 6	Processing of Personal Data
6c	Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
6d	Vital interests: the processing is necessary to protect someone's life.
6e	Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Article 9	Processing of Special Category – Sensitive Data
9b	processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data subject in the field of employment and social security and social protection law
9c	processing is necessary to protect the vital interests of the Data subject or of another natural person where the Data subject is physically or legally incapable of giving consent;
9g	processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued

5.2 Fair processing is the responsibility of each controller to ensure by the issuing of a privacy notice that all data subjects are aware of what, why and how their data is processed.

6. Access and individual's rights

6.1 The parties acknowledge that data subjects have rights under Articles 12 through to Article 22 of the GDPR. The parties will deal with the exercise of subject rights in accordance with the requirements of the GDPR and relevant data protection legislation. Both parties must have appropriate policies and procedures in place which allow these rights to be exercised by the data subject. The parties undertake to keep each other advised of the exercise of subject rights in relation to data shared under this protocol.

6.2 To comply with fairness and transparency requirements, it is the responsibility of each party to ensure that their privacy notice(s) or fair processing notice(s) properly reflect their data sharing arrangements in accordance with the requirements of Articles 13 and 14 of the GDPR.

6.3 Freedom of Information Act 2000 (FOI) requests and data protection subject access requests:

6.3.1 Any request for information made under the FOI must be notified to the party who is the controller of the data, within 3 working days, in order to fulfil the 20 working days FOI legislation.

6.3.2 Any subject access request made under data protection legislation must be notified to the party who is the controller of the data, within 3 working days, in order to fulfil the one month GDPR legislation.

6.4 Where a subject access request involves personal information received from a controller not party to this Agreement, the receiving party shall determine whether they need to contact the other who initially shared the data, to advise them accordingly and seek any representations, including whether an exemption to disclosure should apply. However, the decision to disclose rests with the receiving party.

6.5 Where a data subject exercises their right to rectification, erasure or restriction with regard to data shared under this Agreement, the party who shared the data must notify the receiving party of the outcome of the request. The parties shall under this protocol, have appropriate mechanisms and procedures in place to effect any amendments required, including the addition of a supplementary statement and the provision of support to assist investigations and other legal requirements.

6.6 Where a data subject exercises their right to object, the party receiving the complaint shall notify the Data Protection Officer (DPO) of the relevant party within three working days. The parties must have appropriate mechanisms and procedures to cease processing of the specified Data whilst the validity of the request is assessed. If the request is upheld there must be no further processing of the data.

6.7 Where any complaint or claim arises that there has been a breach of data subject's rights or the controller obligations, the party receiving the complaint shall notify the DPO of the sharer organisation immediately. Notification may be by telephone or email and

assist in anyway possible with investigation, recommended actions or requirements arising from such complaints or breaches.

7. Keeping Data secure and confidential

- 7.1 The parties must maintain policies and procedures which govern the processing of information and ensure that all activity is undertaken in accordance with the principle of integrity and confidentiality under Article 5 of the GDPR.
- 7.2 The parties shall implement appropriate technical and organisational measures to protect the data from any unauthorised or unlawful processing or accidental loss, destruction or damage in line with the obligations of a data controller. These measures must be:
 - 7.2.1 Compliant with national data security requirements, standards and or certification such as ISO/IEC 27001:2005 (ISO/IEC 17799:2005) as appropriate to the data being shared under the protocol; and
 - 7.2.2 Fully and diligently followed and applied with by their agents at all times; and
 - 7.2.3 As a minimum, attain the required standards of data protection legislation.
- 7.3 The parties will ensure that their personnel, including temporary and contract employees, are able to access only the shared information necessary for their role.
- 7.4 The parties will ensure that their personnel, including temporary and contract employees, receive appropriate data privacy and security training and are subject to appropriate confidentiality and non-disclosure obligations.
- 7.5 The parties shall ensure that electronic copies of the data are only ever held on encrypted devices or servers and are not e-mailed un-securely. Any portable devices must be encrypted and data should not be transferred onto unsecure portable devices. When data is no longer required it must be disposed of securely and permanently in accordance with this protocol and or any binding retention or archiving requirements and codes of practice.
- 7.6 The parties shall ensure that all paper copies of shared information under this Agreement, held by it are secure and in the event of transfer, securely transferred either by safe haven fax or couriered in sealed and appropriately labelled containers and shredded upon disposal.
- 7.7 Neither party may pass on the data to third parties without an appropriate lawful basis under the GDPR. If data is shared with third parties who are not a party to this Agreement, the sharing party is responsible for ensuring that there are appropriate data sharing arrangements and it is done in accordance with the requirements of the GDPR and Data Protection Legislation.
- 7.8 The parties are responsible for ensuring that there are appropriate data processing agreements in place if third party processors are used. Any data processing agreements must ensure there are sufficient provisions to meet the GDPR requirements and protect

data subject rights. The parties are required to ensure any sub-contractors they use are managing all aspects of data security and are fully aware of and abide by this Agreement.

- 7.9 Any data breaches involving data shared under this Agreement for example: theft, loss, damage, unauthorised access or inappropriate disclosure of data must be reported to the DPO of the other party as soon as possible.
- 7.10 The parties must ensure that no data is transferred or hosted outside the European Economic Area. This clause binds processors and sub-processors acting on behalf of the Parties.

8. Record of Processing Activity

Both parties are responsible for keeping accurate records of data processing activity, including the sharing of data pursuant to this Agreement.

9. Data accuracy, retention and deletion

- 9.1 If data is found to be inaccurate, it is the responsibility of the party who discovered the inaccuracy to notify the other who shared the data.
- 9.2 The shared data will be retained in accordance with the data protection legislation requirements. The parties must have an appropriate retention schedule in relation to the retention and deletion of shared data.
- 9.3 Subject to any statutory retention requirements, once the reasons for sharing the data have been satisfied the data should be securely destroyed. All relevant data must be deleted from computer systems (including, but not limited to; personal computers, laptops, other computers, electronic handheld devices, memory sticks, USB sticks, servers, hard drives, CD ROMs, and other forms of media storage inclusive of cloud storage) and any hard copies.

10. Complaints

Both parties will use their data privacy complaints procedures to deal with complaints from the public arising from sharing data under this Agreement.

11. Data Breach

- 11.1 If a data breach is found to have occurred, it is the responsibility of the party who first becomes aware of the breach to notify the other party who will ensure the circumstances and data breach detail is documented, reported appropriately and the necessary reporting requirements and timescales within the regulations are adhered to.
- 11.2 The parties are responsible for having appropriate measures in place to manage data security breaches including identifying, investigating and dealing with unauthorised access to, or use of, data shared under this protocol.

12. Changes and Termination to Terms of Agreement

The parties reserve the right to change or terminate the terms of this agreement by notifying the other party in writing and in any case not less than 30 days from the date of the written notice.

13. Jurisdiction

The Agreement shall be governed in accordance with the law of England and Wales, under the Supervisory Authority of the Information Commissioner's Office and competent Courts of Law in England and Wales.

14 Disputes

- 14.1 The Parties shall make every reasonable effort (acting in good faith at all times) to resolve by agreement any dispute which arises between them about any issue relating to this Agreement.
- 14.2 If the Parties are unable to reach a mutually satisfactory resolution of their dispute within 10 Business Days of a dispute being notified in writing by one Party to the other, then the Parties shall comply with the following procedures:
- 14.2.1 The issue shall be discussed at a meeting, at which the Parties' authorised representatives will attend, to be held within 10 further Business Days;
- 14.2.2 If the dispute is not resolved within a further 10 Business Days after the above meeting, the issue shall be referred to senior managers for both Parties;
- 14.2.3 If the Parties' senior managers fail to resolve the dispute within 10 Business Days of its referral to them, either Party may refer the dispute in accordance with the Centre for Effective Dispute Resolution ('CEDR') Model Mediation Procedure;
- 14.2.4 If the Parties do not agree on the identity of the mediator then either Party may ask CEDR to appoint a mediator;
- 14.2.5 The Parties must pay the mediator's fees in equal shares (unless otherwise agreed)


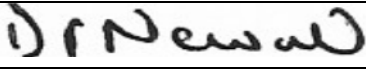
and do whatever possible to ensure that the mediation starts as soon as possible.

- 14.3 Any agreement reached as a result of mediation under this section shall be final and binding upon the Parties, but if the dispute has not been settled within 20 Business Days of the mediation starting then either Party may instigate court proceedings.
- 14.4 Use of the above dispute resolution procedure shall neither delay nor take precedence over any use of this Agreement's default or termination procedures.

15 Notices

- 15.1 All notices under this Agreement must be sent via designated email accounts, or first class, or recorded delivery post, or delivered by hand.
- 15.2 Any notice to the Parties shall be addressed to their respective authorised representatives at the designated physical or email addresses stated in the Contract.

Signatories

SMBC Signatory	Brushstrokes Signatory
Designation: Director of Law and Governance & Monitoring Officer	Designation: Project Manager
Name: Surjit Tour	Name: Dave Newall
Signature: 	Signature: 
Date: 24 September 2020	Date: 22.9.20