London Borough of Southwark

Southwark Works Employment Support Framework

Section 10 – Information Sharing Agreement

Southwark Works Framework Information Sharing Agreement

1. Definitions

1.1 **"Information"** means:

a) Personal Data
b) (as defined in Article 4 of the UK GDPR, Part 1 (3) of the DPA 2018 and any subsequent data protection legislation)
c) Information subject to a duty of confidence.
d) Sensitive or Special Category Personal Data (as defined in Article 9 of the UK GDPR, Part 2, Chapter 2, Section 10 of the DPA2018 and any subsequent data protection legislation).
e) Private information (for example; information relating to a person's private and family life, his home and his correspondence, in accordance with Article 8 of the Human Rights Act 1998).

2. Purpose and Background

2.1 This Agreement defines the specific arrangements for sharing Personal Data, Special Category and Personal Data (the 'Information') between Southwark Council and the signatory organisations below in respect of the Southwark Works Programme.

2.2 In order to share appropriate Information between partners there must be a lawful, defined and justifiable purpose(s) which supports the effective delivery of a policy or service that respects people's expectations about the privacy and confidentiality of their Information but also considers the consequences of a failure to act. This in turn must be supported by robust business processes.

2.3 If this Information Sharing Agreement links in with any other Information Sharing Agreements or contracts please state which:

Hanlon Customer Relationship Management contract
Pre apprentice support contract

3. Details of Information Sharing

3.1 ***What is the purpose of the Information sharing? What is it meant to achieve?***

Southwark Works is being delivered by a Framework of providers and a Network Coordinator in the London Borough of Southwark. The primary purpose of the programme is to provide clients support to help improve their chances of finding work through a caseworker model. The purpose of appointing a Framework of providers is to ensure that clients receive the best service tailored to meet their needs. The programme will do this by working in partnership across the Framework of providers, network coordinator and CRM system providers; referring clients to the most appropriate provider. The Southwark Works programme relies on the ability of providers to use a central CRM system; this allows providers to allocate clients across the network. Using

the central CRM system encourages a more streamlined service as clients do not need to repeat their information and caseworkers do not need to waste time in creating new client files.

Southwark Works service providers also work with local services; referring clients to other support services such as those provided by Southwark Council, Job Centre Plus, health service providers and the voluntary and community sector.

In order to ensure that clients are able to get the best support possible, Southwark Works provider (specified in 3.2) caseworkers may need to share information with these services.

3.2 ***What are the potential benefits and risks to individuals and / or society of sharing or not sharing the Information?***

The primary benefit is to provide specialised services in supporting unemployed clients or clients with specific difficulties in finding suitable work and at the same time increasing their feelings of wellbeing and inclusion. Not sharing data about vulnerable clients could mean that they will not receive the best possible employment support.

Southwark Works providers will endeavour to minimise the risk by only providing information that is key for any third party to provide its specialist services and will only use predefined services to deliver this support.

The risk of not sharing data between providers will be a disjointed service where clients are required to complete multiple registration documents, share their employment history and related information (such as CV, right to work) many times.

There are risks associated with sharing data and potential external threats to the security of the data. Referring to paragraph 3.13; all parties to this agreement will put the relevant mitigating factors in place.

3.3 ***What Information is being shared?***

Data type	**Will this be shared? (Y/N)**	**Is Information anonymised or pseudonymised? If not, why not?**
Personal Data		
Full name	Y	No – as this specific data is required to identify client and support them
Address	Y	No (as per reason above)
Contact details	Y	No (as per reason above)
Date of Birth	Y	No (as per reason above)
National Insurance number	Y	No (as per reason above)
Employment status	Y	No (as per reason above)
Right to work status	Y	No (as per reason above)
Qualifications	Y	No (as per reason above)
Housing status	Y	No (as per reason above)

Income / benefit status	Y	No (as per reason above)
Whether any dependants or caring responsibilities	Y	No (as per reason above)
Referral source	Y	No (as per reason above)
Special Category Information		
Ethnicity	Y	No (as this specific data is required to identify gaps in service provision)
Gender	Y	No (as this specific data is required to identify gaps in service provision)
Religion	N	N/A This specific data is not collected
Health (including disability)	Y	No (as this specific data is required to identify gaps in service provision)
Sexuality	N	N/A This specific data is not collected
Criminal record	Y	No (as this specific data is required to identify gaps in service provision)
Political opinions	N	N/A This specific data is not collected
Trade union membership	N	N/A This specific data is not collected
Case notes	Y	No (as this specific data is required to deliver effective services)
Confidential or Private Information		
Other – specify	N	N/A

3.4 ***What is your legal justification for sharing?***

Does your organisation have the power to share and if so under what legislative function? Include which Article 6 and Article 9 of the UK GDPR conditions are met; if you're interfering with Article 8 of the Human Rights Act 1998, include the justification; if you're overriding the Duty of Confidentiality state the justification.

The legal justification for sharing is given under Article 6 (1) a and c and Article 9 (2) b of the General Data Protection Regulation. (*Article 6 (1) a:, the data subject has given consent to the processing of his or her personal data for one or more specific purposes; and Article 9 (2) b: Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or… subject on the field of employment, social security or social protection law…providing for appropriate safeguards for the fundamental rights and interests of the data subject.*)

See also Part 2, Chapter 2, Section 8 of the Data Protection Act 2018.

The Council may process data for the purposes of this programme in exercise of the general power of competence under section 1 of the Localism Act 2011 and powers under section 111 of the Local Government Act 1972. These provisions, respectively, give the Council the power to do anything individuals generally may do (subject to the limitations set out in the Localism Act 2011), and the

power to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of the functions of the local authority.

3.5 ***Is an individual's consent required before you can share the Information?***

If not, then please provide justification as to why not. If yes, please explain when and how consent will be obtained and recorded. Has the purpose of the sharing been covered off in your privacy notice?

Consent of the data subject is required for the sharing and processing of this data.

Southwark Works clients are made explicitly aware that their data will be shared with Southwark Council (as commissioner of the service) and other Southwark Works service providers in order to provide them the best possible support. This will be done at point of registration through a privacy notice which the service user is required to sign.

3.6 ***How will the Information be transmitted to the receiving Party and how will the receiving Party store the Information?***

Outline how the Information will be transmitted and which database(s), system(s) or location(s) it will be transferred between. Ensure adequate security is in place to protect data during transmission, e.g. data transfer / secure email / restricted access to authorised personnel. Outline how the information will be stored by the receiving Party, e.g., secure server - include any security measures.

Client data is recorded and stored on the CRM system.

The CRM system is commissioned by the council. All providers have access to the CRM; however individual client data is restricted to the organisation(s) with whom the client is currently working.

Each provider can only see the clients who have been referred to them. Providers can refer clients to another provider, whilst keeping their referral open (for example: the records of an ex-offender with a mental health need may be open to Provider A, Provider B and Provider C as they are all working with the client. However, other providers would not be able to access this record).

For clarity, the CRM system provider acts as a processor of data and all providers using the Southwark Works CRM system act as distinct data processors. The council is the data controller.

Information is not transferred outside of the CRM system, and it is not anticipated that any personal data would be processed separately from the CRM system. This ensures that there is no external 'transfer' of data between providers.

Access to the CRM system is restricted to named personnel, and access to all user data is fully auditable.

What method will be used by the disclosing Party for secure transmission?	What method will the receiving Party use to securely store the Information once received?
Hanlon CRM system	Hanlon CRM system
Secure email communication	

3.7 ***Who will be responsible for ensuring safe handling of the Information?***

Information should only be shared with and accessed by those who have a legitimate need to know for the purpose of this Information Sharing Agreement. They must be adequately trained in Information Governance, data protection and confidentiality.

Name	Role	Organisation	Contact Details
Liz Gardiner	Senior Strategy Officer	Southwark Council	liz.gardiner@southwark.gov.uk
SERVICE PROVIDER DETAILS TO BE CONFIRMED			

3.8 ***Who will be the Data Controller for the purposes of the Information being shared?***

Please clarify below who the Data Controller is for the Information being shared as listed at question 4.3.

Southwark Council is the data controller for data processed through the Southwark Works service. The CRM provider and Southwark Works service providers are data processors.

3.9 ***What arrangements will be in place to facilitate data subjects to exercise their rights under the relevant legislation (for example; subject access, restriction, rectification)?***

Southwark Works service providers will implement a standard Subject Access Request, restriction and rectification policy.

Data subject rights

In accordance with data protection legislation, all data subjects have the freedom to apply their rights to information held by all parties.

Data subjects may approach any party to apply the following rights:

- Inform

- Access
- Rectification
- Erasure
- Restriction
- Data portability
- Object
- Automated decision profiling

All requests received by any party must be actioned in accordance with the relevant party's data protection policy. In line with legislation, data rights requests must be responded to within one calendar month of them being received. Parties who have received a data access request relating to the Southwark Works service will notify the council at the earliest possible time, at least within in 5 working days.

If a request for access is received from a relevant data subject, all parties must assist, where appropriate, to retrieve the information requested. Requests must be handled through each party's own subject access request/data protection policies and guidance.

If a request for rectification is received from a data subject, a party will inform the council of the request and any amendments made. Where a request has been received by all relevant parties and a decision has been made not to amend the data, the council will note on the record that:

- A request has been received
- The date the request was received
- The decision to not amend the data has been applied
- The date the decision was made.

If a data subject right request is escalated to the Information Commissioner's Office (ICO), all relevant parties agree to keep each other informed and to provide the outcome.

All parties understand that this agreement and information shared within the agreement may also be subject to further access to information legislation. The information received may be subject to, but not limited to, requests made under the Freedom of Information Act 2000, the Environmental Information Regulations 2004, the UK GDPR and the Data Protection Act 2018. All parties agree to assist the council in undertaking its legal duties pursuant to the aforementioned acts.

3.10 ***How long will the Information be kept?***

There should be agreed retention periods for the data.

In line with the 'audit and records' clauses of the Southwark Works Framework Agreements, anonymised data will be kept for the Framework Term and for six years thereafter.

In line with schedule 16 of the Network Coordination service contract, anonymised data will be kept for the contract term and six years thereafter.

3.11 ***How will the Information be destroyed?***

The Information should be destroyed securely and certification produced where possible to prove this has happened.

Information will be destroyed in accordance with the council's protocols. Personal information will be anonymised two years from contract end.

3.12 ***What date will the Information be shared and how often?***

Initial date must be later than the date of the signatures in section 3 above and should give an indication of subsequent dates for regular sharing.

Not before the commencement of this data sharing agreement. Data will only be shared during the period that is beneficial in providing the required services to the client, and in accordance with Southwark Works contractual requirements. Sharing will be on an ad hoc basis, as and when relevant for casework.

3.13 ***In the course of sharing the Information, what could go wrong, why could it go wrong and how will the Parties stop this from happening?***

Southwark Works service providers mitigate the risk of not sharing safely and securely by having processes in place that are reviewed as part of their ISO9001 processes as well as reviewing incident and risk registers. Southwark Works providers have a Security Incident Reporting Procedure, which would be followed for any breaches. Staff undertake Data Protection Training, prior to gaining access to client data and systems. Each organisation has its own procedures for addressing incidents and each organisation confirms by signing this agreement that they ensure their staff are trained in data security and follow the procedures which apply locally for secure sharing. Learning from any incidents should be shared with Southwark Council so as to improve processes across the Southwark Works service. Breaches must be reported by Southwark Works providers or the CRM system provider to Southwark Council under the contract.

3.14 ***When will this agreement be reviewed and by whom?***

Name	**Review date (should be at least every 12 months)**
Southwark Council and Southwark Works Framework providers	Annually until the end of the Southwark Works Framework (July 2027)

4. Termination

4.1 Any Party may withdraw from this Information Sharing Agreement:

i) upon giving a minimum of three month's written notice to the other Parties to the Information Sharing Agreement; or

ii) immediately where any term(s) of the Information Sharing Agreement or Overarching Protocol has been breached.

4.2 Information which is no longer relevant should be confidentially destroyed or returned to the Disclosing Organisation. The withdrawing Party must continue to comply with the terms of this Information Sharing Agreement in respect of any Information that the Party has obtained through being a signatory.

Appendices:	
1	Privacy notice
2	Data breach process
3	

5. Parties to this Information Sharing Agreement

5.1 This Information Sharing Agreement must be formally approved and signed by the Parties to enable Information Sharing to take place by persons with authority to do so on behalf of their organisation. The Parties will ensure that this Information Sharing Agreement and any associated documents are known and understood by all staff involved in the process.

5.2 This Information Sharing Agreement may be executed in any number of counterparts each of which when executed shall constitute a duplicate of the original, but all the counterparts shall together constitute the Agreement. No counterpart shall be effective until each Party has executed at least one counterpart.

Party Name	**London Borough of Southwark**
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	**Hanlon (CRM)**
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	

Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory/Date	
Date of agreement	

Party Name	
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	

Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	
Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	

Party Name	

Data Protection Registration Number	
Address	
Responsible Manager	
Contact Details	
Authorised Signatory	
Date of agreement	