Data Protection Impact Assessment

What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment ("DPIA") is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies. Projects of all sizes could impact on personal data.

The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Conducting a DPIA should benefit the Council by producing better policies and systems, and improving the relationship with individuals.

Why should I carry out a DPIA?

Carrying out an effective DPIA should benefit the people affected by a project and also the organisation carrying out the project.

Not only is it a legal requirement in some cases, it is often the most effective way to demonstrate to the Information Commissioner's Officer how personal data processing complies with data protection legislation.

A project which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A DPIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

When should I carry out a DPIA?

The core principles of DPIA can be applied to any project that involves the use of personal data, or to any other activity that could have an impact on the privacy of individuals.

Answering the screening questions in Step 1 of this document should help you identify the need for a DPIA at an early stage of your project, which can then be built into your project management or other business process.

Who should carry out a DPIA?

Responsibility for conducting a DPIA should be placed at senior manager level. A DPIA has strategic significance and direct responsibility for the DPIA must, therefore, be assumed by a senior manager.

The senior manager should ensure effective management of the privacy impacts arising from the project, and avoid expensive re-work and retro-fitting of features by discovering issues early.

A senior manager can delegate responsibilities for conducting a DPIA to three alternatives:

a) An appointment within the overall project team;
b) Someone who is outside the project; or
c) An external consultant.

Each of these alternatives has its own advantages and disadvantages, and careful consideration should be given on each project as to who would be best-placed for carrying out the DPIA.

How do I carry out a DPIA?

Working through each section of this document will guide you through the DPIA process.

The requirement for a DPIA will be identified by answering the questions in Step 1. If a requirement has been identified, you should complete all the remaining sections in order.

After Step 5, the Information Lawyer (Data Protection Officer) will review the DPIA within 14 days of receipt, and complete the rest of the assessment within 28 days. The DPO will identify any privacy risks, and proposed measures to address them.

These measures must then be agreed by the project lead, Information Asset Owner or Administrator, and, in some cases, the Senior Information Risk Owner.

Advice can be found at the beginning of each section, but if further information or assistance is required, please contact the Information Lawyer (Data Protection Officer) on 023 8083 2676 or at information@southampton.gov.uk.

Data Protection Impact Assessment Template			
Version	3.1	**Approved by**	Data Protection Officer
Date last amended	2nd November 2018	**Approval date**	2nd November 2018
Lead officer	Chris Thornton, Information Lawyer (Data Protection Officer)	**Review date**	2nd November 2019
Contact	information@southampton.gov.uk	**Effective date**	2nd November 2019

Project Details

Name of Project
Integrated Advocacy service
Brief Summary of Project
The project aims to commission a new Integrated Advocacy service for Southampton, replacing an existing commissioned service, whose contract expires on 31st March 2020. Once commissioned, the new service will provide a holistic Integrated Advocacy service that will meet the needs of all eligible individuals within Southampton. This will include individuals of all age groups with learning disabilities, autism, mental health issues, physical and sensory disabilities and long term conditions.
Estimated Completion Date
1.4.2020
Name of Project Lead
Amanda Luker, Senior Commissioner

Details of Person Conducting DPIA

Name
Jackie Hall
Position
Commissioner
Contact Email Address
Jackie.hall@southampton.gov.uk

Step 1: Identify the need for a DPIA

Does your project involve… (tick all that apply)
☒ The collection of new information about individuals
☐ Compelling individuals to provide information about themselves
☒ The disclosure of information about individuals to organisations or people who have not previously had routine access to the information
☐ The use of existing information about individuals for a purpose it is not currently used for, or in a way it is not currently used
☐ Contacting individuals in ways which they may find intrusive
☐ Making changes to the way personal information is obtained, recorded, transmitted, deleted, or held
☐ The use of profiling, automated decision-making, or special category data[1] to make significant decisions about people (e.g. their access to a service, opportunity, or benefit).
☐ The processing of special category data[1] or criminal offence data on a large scale.
☐ Systematically monitoring a publicly accessible place on a large scale.
☐ The use of new technologies.
☐ Carrying out profiling on a large scale.
☐ Processing biometric or genetic data.
☐ Combining, comparing, or matching data from multiple sources.
☐ Processing personal data without providing a privacy notice directly to the individual.
☐ Processing personal data in a way which involves tracking individuals' online or offline location or behaviour.
☐ Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
☐ Processing personal data which could result in a risk of physical harm in the event of a security breach.

[1] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

If you answered "yes" to any of these, please proceed to Step 2.
If none of these apply, please tick the below box, and return the form to the Information Lawyer (Data Protection Officer) at information@southampton.gov.uk
☐ None of the screening statements in Step 1 of this document apply to the project, and I have determined that it is not necessary to conduct a Data Protection Impact Assessment

Step 2: Describe the processing

The nature of the processing

How will you collect data?

The provider will collect information from referrals received (sources identified in the section above). Southampton City Council and other referring agencies (including self-referrals or referrals from carers, friends, members of the public) will send information via the prescribed referral routes.

The provider will be a data controller.

The provider will use information received in order to make contact with referred individuals in order to offer appropriate advocacy services. Service users may be eligible for more than one statutory advocacy service in additional to non-statutory advocacy so may seamlessly move between different elements of the service. For example a service user may be referred for an IMCA due to lacking capacity to make the decision to move from general hospital to residential care. Inherent within that there may be a requirement to assess their needs under the Care Act 2014 and so they may also be eligible for Care Act advocacy as well as for an Independent Mental Capacity Advocate. The provider will make decisions on eligibility for aspects of the service based on information received in the referral and additional information gathered in its own assessment of the individual's circumstances.

Personally identifiable information (PII) will only be shared by the provider with others where it is necessary in order to advocate on their behalf and where they have the consent of the service user to do so (or where they have a lawful basis to do so e.g. under the Mental Capacity Act in order to fulfil the advocacy role).

No PII will be shared with Southampton City Council except by exception (for example to report a safeguarding adults or safeguarding children's issue). This will be on a case by case basis and via the most appropriate method (e.g. phone call or secure email to the MASH team or to the allocated social worker). Anonymous service usage data will be shared with the commissioner on a quarterly basis. This does not contain any PII.

Southampton City Council is not prescriptive on how the provider will store information – only that its systems for doing so are compliant with GDPR. The contract will also specify compliance with record retention lengths and the requirement to delete information once retention periods have been met.

The highest data processing risk is the sending of PII information via non secure email either from referrer to the provider or from the provider to another agency. The provider will be required to ensure that they send information securely and referral information will make clear that information must be sent securely to them or if that is not possible to refer by phone. The potential for an online web based referral form removing the necessity for referrals via email will be explored with the new provider.

The provider may receive a referral for an adult with capacity to make a decision about the receipt of advocacy services where they have not provided consent to be referred.

The contract will need to ensure that the provider has procedures in place to check that informed consent was provided before referral and to check on first contact with individuals that they have consented to the referral.

If the individual states that they did not/do not consent to the referral – the provider will have systems in place in order to delete all information held on that individual unless there is a lawful basis to proceed without consent (for example the individual lacking capacity to make the decision on consent – and a best interests decision under the Mental Capacity Act affirms the necessity to proceed).

If the client has consented and withdraws their consent for their information to be held/processed by the provider – then the provider will need to ensure that they have systems in place to manage this scenario and delete the individual data. Additionally appropriate mechanisms will be required to capture anonymous service usage data if the service user has received an advocacy service prior to consent being withdrawn.

Where appropriate and the service user has capacity, advocates are encouraged to complete an Advocacy Agreement form with their clients, setting out the issues that will be dealt with by the advocate. This document can be reviewed at any time, and advocates are always clear with service users about the issues they can and can't deal with. Wherever possible, if an issue is not appropriate to be dealt with by an advocate, the service user will be signposted to another agency.

Individuals will be asked to complete a permission to share agreement at the point of engagement with the service and at regular intervals thereafter, but no less than annually.

Information will be held in accordance with the commissioned providers data protection policies, which in turn will be compliant with the terms and conditions of the contract.

How will you use the data?

Data will be used to offer an appropriate Advocacy service to eligible individuals who require it.

The Service will protect the confidentiality of all individuals receiving support whilst ensuring that information is shared where required within relevant safeguarding and operational policies as outlined within the Terms and Conditions to this Agreement.

How will you store the data?

Personal data will held by the providers. Storage will be, at a minimum compliant, with relevant legislation as set out in the terms and conditions of the contract. Providers will hold electronic and paper files to support the delivery of integrated advocacy services.

A number of IT systems or applications are available to providers. The specific system will be secured by the provider once the contract is awarded. IT systems will need to reflect the requirements as set out in the service specification.

How will you delete the data?

Retention periods and the destruction of personal data will be set by the providers own data protection policies but will be, at a minimum compliant, with relevant legislation as set out in the terms and conditions of the contract.

If the individual states that they did not/do not consent to the referral – the provider will have systems in place in order to delete all information held on that individual unless there is a lawful basis to proceed without consent (for example the individual lacking capacity to make the decision on consent – and a best interests decision under the Mental Capacity Act affirms the necessity to proceed).

If the client has consented and withdraws their consent for their information to be held/processed by the provider – then the provider will need to ensure that they have systems in place to manage this scenario and delete the individual data. Additionally appropriate mechanisms will be required to capture anonymous service usage data if the service user has received an advocacy service prior to consent being withdrawn.

What is the source of the data?

The source of the data will be the individual requiring the Advocacy service or member(s) of their family if appropriate.

Will you be sharing data with anyone?

INFO: If yes, please provide details

Individuals engaging with the service will asked to complete a permission to share form, which will set out the agencies and individuals with whom their information can be shared. The collection and sharing of information will be compliant with the terms and condition of the contract awarded to the provider by the city council.

At the first meeting with an advocate, confidentiality, information storage and information sharing will be discussed and agreed with the service user. The Permission to Share/Confidentiality form will be completed and signed. Where service users do not have capacity to understand or agree, advocates will follow the providers guidance and policy relating to sharing information. Advocates endeavour to secure permission to share and/or consent in accordance with GDPR and all data protection legislation.

If the Advocate is unable to gain permission from the client due to capacity issues or communication difficulties, they can ascertain the need to share on a best interest basis according to the Mental Capacity Act Code of Practice Guidance.

Service users are reminded about the limits of confidentiality at the beginning of every meeting with their advocate.

The Permission to Share agreement is reviewed when/if circumstances change, e.g. the service user wants information shared or withheld with a person or service not detailed on the form, or a new issue is identified. The service user has the right to withdraw permission to share with any party previously identified at any time (excluding disclosures made due to safeguarding concerns).

Information, via the permission to share protocol, is likely to be shared with health professionals (GP's, community nurses, hospital staff) and adult social care representatives (social workers).

Describe the scope of the processing

What is the nature of the data?

INFO: Detail the type of personal data being processed. List any fields that will be processed (e.g. name, address, data of birth, NHS number, video images)

The data collected is used to provide an advocacy service for the service user and as such includes the following, either to determine eligibility for the service or required in order to advocate effectively on behalf of the service user. The information required for referral to the service does include special category data:

- Name
- Date of Birth
- Address
- Contact details (eg phone number).
- Ethnicity
- Care Group (mental health, learning disability, autism, substance misuse, older person, physical disability or sensory impairment, carer (including young carer), young person aged 16-18 in transition to Adult Services).
- Details of the issues that the person requires advocacy support with.
- Details of their "substantial difficulties, including any communication difficulties and reasonable adjustments you have already made for them" (Eligibility question to determine whether they meet the criteria for an advocate).
- Referrer's details (name, contact details).
- Details of any professionals (including any existing advocates) involved with the person and any family/friends actively involved in their care.
- Any risks or behaviours that may affect lone working.

Data will be collected following every referral to the service.

- Data will be retained as per GDPR guidelines. Where a referral is made without the consent of the individual and where no legal basis exists to process that referral without consent, the provider will make contact with the individual to seek their consent. Where consent is refused the provider will immediately delete the individual's records.
- The contract covers all areas of Hampshire.
- Data will be collected on all referred eligible service users.

- The current contract provided an advocacy service to 4909 individuals in the 2018/19 financial year (not including the Independent Health Complaints Advocacy Service which is not yet part of this contract). The current provider has confirmed that this figure is representative of the yearly level of demand across the last 4 years.

The Independent Health Complaints Advocacy Service has supported 112 individuals in the last 6 months. Assuming demands remains constant this would equate to approximately 224 individuals on an annual basis.

Does it include special category or criminal offence data? Please provide details.

INFO: "Special category" data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data concerning health, both mental and physical.

How much data will you be collecting and using?

Data collected will be proportionate with the needs of the individual. All data collected is proportionate and relevant to the service being provided.

The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the contract. The terms and conditions of the contract clearly sets out the requirements to be compliant with data protection laws, including ensuring that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed is collected.

How often will the data be collected and used?

Data will be collected and recorded as often as the individual in receipt of the service is seen by the Advocate. Frequency of visits will be variable depending on the needs of the individual and the complexity of the case.

How long will you keep it?

Retention periods will be set by the providers own data protection policies, but will be, at a minimum compliant with relevant legislation as set out in the terms and conditions of the contract.

If the individual states that they did not/do not consent to the referral – the provider will have systems in place in order to delete all information held on that individual unless there is a lawful basis to proceed without consent (for example the individual lacking capacity to make the decision on consent – and a best interests decision under the Mental Capacity Act affirms the necessity to proceed).

If the client has consented and withdraws their consent for their information to be held/processed by the provider – then the provider will need to ensure that they have systems in place to manage this scenario and delete the individual data. Additionally

appropriate mechanisms will be required to capture anonymous service usage data if the service user has received an advocacy service prior to consent being withdrawn.

How many individuals are affected?

Below is the number of service users currently being dealt with by the service but this is likely to change with the new Liberty Protection Safeguards legislation that is due to come into force in Autumn 2020.

Period	**Referrals received**	**Number per month**	Percentage increase	
			From contract start	from last period
2015/16	461	38.41	n/a	n/a
2016/17	647	53.91	40.35%	40.35%
2017/18	883	57.58	91.54%	36.48%
2018/19	849	70.75	84.16%	-3.85%

What geographical area does it cover?

Southampton City

Describe the context of the processing

What is the nature of your relationship with the individuals?

INFO: Detail who the data subjects will be (e.g. residents, carers, pupils, staff, professionals)

The overriding purpose of an Advocacy service is to enable individuals to take more responsibility for themselves and reduce their dependency on other people. Empowering individuals to self-manage and to take control of their own lives will be central to the advocacy support provided as part of this Service.

The Service will support and develop the ability of individuals to self-advocate, increasing their confidence and assertiveness skills and enabling them to support themselves as far as is possible in future. This will include providing the opportunity for individuals to train as peer/volunteer advocates, offering additional support to local people.

The Service will adhere to principles of personalisation and will be delivered flexibly in a way that offers choice and control to individuals with regards to the advocacy support that they receive, recognising that those receiving support have the most specialised knowledge of their needs.

The Service will be accessible to the wide diversity of communities within Southampton, respecting people's culture and religious beliefs and making reasonable adjustments to ensure that no individual will be excluded from accessing services on the grounds of ethnicity, culture, religion, class, gender, sexual orientation, disability, age, marital status or caring role.

The Service must establish links and work in partnership with others including public, independent and voluntary sector agencies to improve the overall quality and effectiveness of wider support services within Southampton.

The Service must assist individuals, staff, carers and agencies who are likely to make referrals to the Service to understand the role of advocates, with an emphasis on statutory elements of provision, in order for them to know how and when to access the service. This will include a targeted communications and publicity programme at the start of the contract.

The Service will protect the confidentiality of all individuals receiving support whilst ensuring that information is shared where required within relevant safeguarding and operational policies as outlined within the Terms and Conditions to this Agreement.

How much control will they have over their data?

Individuals will be asked to complete a permission to share agreement at the point of engagement with the service and at regular intervals thereafter, but no less than annually.

Consent to share information may be withheld in regards to specific areas of information, for example financial circumstances, or restrictions placed on who the information can be shared with, for example local voluntary agencies. This will be recorded and complied with by staff providing the service.

Individuals will be able to update and amend data at any time during the period that advocacy is requested and provided.

Would they reasonably expect the Council to use their data in this way?

INFO: Please provide details to support your answer

The provider will be a data controller. SCC will not hold personally identifiable information on service users (unless referrals have been made to Adults Services for assessment/provision of services – separately from any issue relating to this contract).

- All data processing in relation to this contract will be undertaken by the provider.
- The individual would be a recipient of one or more advocacy services from the provider.
- The individual has the option to refuse consent at any time and as such their data would subsequently be deleted (except in the cases of individuals assessed as lacking the capacity to make such a decision and a legal duty to provide the service under the Mental Capacity Act exists, or in the case of children where parental consent may be given).
- The collection and use of data is proportionate to the service being provided and would be expected.
- The service includes provision of advocacy to children and vulnerable adults.
- There are no prior concerns over this type of data processing, it is not novel and there are no issues of public concern.
- Relevant clauses relating to the receipt, processing and storage of data will be contained within the provider's contract.

The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the contract.

The terms and conditions of the contract clearly sets out the requirements to be compliant with data protection laws, including ensuring that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed is collected.
Do they include children or other vulnerable groups?
INFO: If yes, please provide details
Yes. People who are experiencing mental health issues or who lack mental capacity are particularly vulnerable and require a high level of safeguarding in order to ensure that they are offered the right care for their needs. Advocacy helps to ensure that these groups have their voices heard in any decisions made about them and that decisions are made in the best interests of the individual concerned.
Are you aware of any prior concerns over this type of processing or security flaws?
INFO: If yes, please provide details
No
Is the processing novel in any way?
INFO: If yes, please provide details
No. Southampton City Council has a statutory duty to provide advocacy services to its population and a discretionary duty to provide non-statutory advocacy services which are viewed as one mechanism to help meet its obligations under the Care Act 2014 to provide "early intervention and prevention" services. As such this service has been commissioned by Southampton City Council since 2015 and the new service will continue to provide both statutory and non-statutory services. There have been no prior concerns over this type of data processing, it is not novel and there are no issues of public concern.
What is the current state of technology in this area?
There are a number of IT systems that can be used for case recording and case management. The specific system will be secured by the provider once the contract is awarded. IT systems will need to reflect the requirements as set out in the service specification.
Are there any current issues of public concern that should be considered?
INFO: If yes, please provide details
People who are experiencing mental health issues or who lack mental capacity are particularly vulnerable and require a high level of safeguarding in order to ensure that they are offered the right care for their needs. Advocacy helps to ensure that these groups have their voices heard in any decisions made about them and that decisions are made in the best interests of the individual concerned.

Describe the purposes of the processing

What do you want to achieve?

Data will be processed by the provider in 2 main ways:

Purpose One: Provision of an advocacy service to the client:

Use of data in order to make contact with the individual with a view to arranging to meet them to discuss their circumstances, issue(s) they require advocacy for and what their wishes/views are.

Following on from this initial meeting, the data gained will be used in order to be able to advocate on their behalf using the information gained from meeting with them to advocate with relevant other professionals who are directly connected with the issues they require advocacy support with. This may involve discussions with others involved in their care to gain additional information (with their consent, or via a best interests decision where they lack capacity to give consent).

The intended effect for individuals is the receipt of an appropriate and effective advocacy service to support them. The benefits of processing for SCC are the delivery of an effective advocacy service to individuals which meets statutory requirements and assists the individual to effectively communicate their views and wishes.

Purpose Two: Provision of contract monitoring data to SCC:

The provider will collate information on service usage providing SCC with statistics for each element of the service.

No personally identifiable information is contained within the contract monitoring report, however the provider will need to process PII in order to produce the report for SCC.

The information provided is intended to allow SCC to monitor the provision of service delivery, specifically:

- ensuring that the service is being provided to the anticipated number of recipients;
- to monitor trends in service provision;
- receive information on and address any problems identified by the provider in delivering the service - such as:
    - under delivery
    - difficulties with partner agencies that may require commissioner assistance to resolve
    - service demand that exceeds ability to meet;
    - to note any complaints and compliments received by the provider and follow up as necessary
- to report on financial spend against the budget for the elements of the contract which are paid by activity.

For the second purpose – the effect for the individual is that SCC ensures the provider is delivering an effective advocacy service that is meeting assessed advocacy needs. The

benefits of processing for SCC are that it receives information that enables effective contract monitoring to ensure that provider is delivering the service according to the requirements of the service specification and that it is remaining in budget or where budgetary pressures are identified – to enable SCC to work with the provider in order to remain within budget or where this is not possible, to enable the commissioning manager to alert senior commissioners of expected financial pressures on the contract.

More broadly the information provided for effective delivery of an advocacy service to individuals and the effective contract monitoring of the service to ensure that effective delivery will have positive impacts across the health and social care systems as individuals are supported to express their views and achieve their outcomes. This sometimes results in the reporting of safeguarding adults issues which may have otherwise been undetected and also in the reporting of quality issues within provider organisations such as hospitals, residential or nursing homes.

The Integrated Advocacy service is to enable eligible individuals to take more responsibility for themselves and reduce their dependency on other people. Empowering individuals to self-manage and to take control of their own lives is central to the advocacy support to be provided as part of this Service.

What is the intended effect on individuals?

The Service will support and develop the ability of individuals to self-advocate, increasing their confidence and assertiveness skills and enabling them to support themselves as far as is possible in future. This will include providing the opportunity for individuals to train as peer/volunteer advocates, offering additional support to local people.

What are the benefits of the processing – for the Council, and more broadly?

To ensure that the statutory duties of the council are carried out in relation to:

Provision of statutory advocacy for vulnerable adults.

- Independent Mental Health Advocacy (IMHA) as determined by the Mental Health Act 1983 (MHA)
- Independent Mental Capacity Act Advocacy (IMCA), including Deprivation of Liberty Safeguards (DOLS) IMCA, as determined by the Mental Capacity Act 2005 (MCA) and from 1st October 2020 – IMCA for Liberty Protection Safeguards (LPS) as introduced by the Mental Capacity Amendment Act 2019.
- Paid Relevant Person's Representative (Paid RPR), as determined by the MCA
- Care Act Advocacy, as determined by the Care Act 2014

Step 3: Consultation process

Consider how to consult with relevant stakeholders
Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so
We intend to engage with professionals, stakeholders and service users as appropriate as part of an engagement/feedback exercise. This will be completed as soon as possible and before the end of September 2019. A questionnaire will be developed and sent out on-line and by e-mail, inviting responses which can be used to develop the service specification for the new service.
Who else do you need to involve, or have you already involved within the Council?
INFO: e.g. IT services, records management
Procurement, Legal services, Adult Safeguarding, DOLS Team
Do you need to ask your processors to assist?
INFO: Processors are third parties who will process the personal data on our behalf
The current service provider is providing a data report which will be used to assess the volume of work required over a 12 month period 1.10.18 – 30.9.19
Do you plan to consult information security experts, or any other experts?
INFO: Please provide details to support your answer
No, it is not deemed necessary to do so due to the nature of the processing.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures
What is your lawful basis for processing? Please choose <u>one</u> of the following…
INFO: There should generally only be <u>one</u> legal basis for processing.
☒ The data subject has given consent ☐ The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ☐ The processing is necessary for compliance with a legal obligation to which the Council is subject

☐ The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council ☐ The processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party
Does the processing actually achieve your purpose?
INFO: Please provide details to support your answer
The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the contract.
Is there another way to achieve the same outcome?
INFO: Please details to support your answer
All data collected is proportionate and relevant to the service being provided.
How will you prevent function creep?
INFO: Function creep is where data collected for one purpose is used for another purpose over time.
The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the contract.
How will you ensure data quality and data minimisation?
INFO: We should only use the minimum amount of personal data possible to achieve the purpose of the processing.
The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the contract. The terms and conditions of the contract clearly sets out the requirements to be compliant with data protection laws, including ensuring that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed is collected.
What information will you give individuals about the processing?
Individuals will be informed during their first engagement with the service and subsequent meetings whether face to face or over the telephone. The permission to share form will be the responsibility of the commissioned provider, but will be compliant with the requirements set out in the terms and conditions of the contract.
How will you help to support their rights?
INFO: Data subject's rights include the right to access, rectify, erase, port, and restrict their data.
Access to files will be set out in the providers own policies and procedures but will be, at a minimum compliant, with relevant legislation as set out in the terms and conditions of the contract.

The service specification for the contract clearly outlines the services to be provided and contract monitoring processes oversee service delivery – part of which would monitor any expansion in scope (i.e. function creep). Contract monitoring includes service user feedback and the contract monitoring reports will demonstrate whether the provider is collecting information as required by the contract and to the standard expected. The provider by virtue of the clauses within the contract will be expected to comply with GDPR and as such provide information in an accessible format to any individuals who use the service. No international transfers of data would be expected, except perhaps in very rare occasions where an oversees relative/friend decides to make a referral into the service. The chances of this are extremely low and the provider would be expected to ensure that appropriate measures are put in place for the safe transfer of information as per GDPR Individuals will be able to update and amend data at any time during the period that advocacy is requested and provided.
What measures do you take to ensure processors comply with the GDPR, and assist the Council in supporting individuals in exercising their rights?
INFO: E.g. will there be a contract in place with the processor that contains data protection obligations?
The handling, storage and use of information will need to be compliant with the requirements set out in the terms and conditions of the contract. The terms and conditions of the contract clearly sets out the requirements to be compliant with data protection laws, including ensuring that only personal data that is adequate, relevant, and not excessive in relation to the purpose for which it is processed is collected.
How do you safeguard any international transfers of personal data?
INFO: If there are no international transfers involved, please state this
There are no international transfers of data involved.

Step 5: Send DPIA Form to the Data Protection Officer

After completing this part of the form, please send the document to the Information Lawyer (Data Protection Officer) at information@southampton.gov.uk

The DPO will review the information provided, and identify and assess the privacy risks.

Step 6: Identify and assess risks (DPO to complete)

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. N/A – all reasonable privacy risks identified and addressed	Remote Possible Probable	Minimal Significant Severe	Low Medium High

Step 7: Identify measures to reduce risk (DPO to complete)

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5			
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**
1.	N/A – all reasonable privacy risks identified and addressed	Eliminated Reduced Accepted	Low Medium High
Comments from the Data Protection Officer			
I am satisfied that all reasonable privacy risks identified and addressed.			
Comments from the Senior Records Officer			
No comments.			

Step 8: Sign off

Item	Date	Notes
DPO reviewed DPIA and provided advice on:	15th October 2019	DPO should advise on compliance, step 7 measures and whether processing can proceed
Senior Records Officer reviewed DPIA on:	4th September 2019	SRO should advise on records management matters
Measures approved by Project Manager on:	16th October 2019	Integrate actions back into project plan, with date and responsibility for completion
Comments from Project Manager:	No comments.	
Residual risks approved by Information Asset Owner / Administrator on:	6th December 2019	
Comments from IAO / IAA:	No comments.	
Residual high risks approved by the Senior Information Risk Owner on:	N/A	If accepting any residual high risk, consult the ICO before going ahead
Comments from SIRO:	N/A	

Step 9: Review

Item	Date	Comments
DPO reviewed DPIA on:		
Date of next review:		