Data Protection Impact Assessment

Project Details

Name of Project
UK Shared Prosperity Fund and Multiply Programme
Brief Summary of Project
As part of the governments 'Levelling Up' agenda the Department for Levelling Up, Housing and Communities (DLUHC) has conditionally offered the Council £1,544,238 to deliver the UK Shared Prosperity Fund (UKSPF), and The Department for Education (DfE) an allocation of £1,182,512 to deliver the 'Multiply' Programme. The funding for both allocations comes from UKSPF. The combined interventions inform a Cabinet Report on 13th September 2022 • Multiply will be delivered using the existing arrangements for Adult and Community Learning and its DPIA compliance will be as that of existing ACL delivery • UKSPF will be delivered alongside existing regeneration/employment projects and its DPIA compliance will be as set out here; Both interventions will benefit residents in the City by helping to increase the number of people into employment, reduce crime, support local businesses, improve the visitor economy and improve numeracy skills. These feed into the Council priorities
Estimated Completion Date
March 2025
Name of Project Lead
John Connelly

Details of Person Conducting DPIA

Name
John Connelly
Position
Service Manager
Contact Email Address
John.connelly@southampton.gov.uk

Step 1: Identifying the need for a DPIA

Does you project involve the processing of personal data?
"Processing" means collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, combining, restricting, erasing or destroying. It should be integral to the project, and not just incidental to it.
☒ Yes ☐ No
If your project does **not** involve the processing of personal data, tick the declaration at the end of this section. If your project **does** involve the processing of personal data, proceed to the next set of screening questions below.

Does your project involve any of the following? (Not all may apply, tick those that do)
☒ 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
Are you planning to carry out any of the following? (Not all may apply, tick those that do)
☐ Evaluation or scoring ☒ Processing of sensitive data or data of a highly personal nature ☐ Processing on a large scale[1] ☒ Processing of data concerning vulnerable data subjects ☐ Processing that involves preventing data subjects from exercising a right or using a service or contract

[1] "Large scale" can mean the number of individuals involved, the volume of data, the variety of data, the duration of processing, or geographical area.

Do you plan to…? (Not all may apply, tick those that do)
☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people
☐ Process special-category data[2] or criminal-offence data on a large scale
☐ Systematically monitor a publicly accessible place on a large scale
☐ Use innovative technological or organisational solutions
☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit
☐ Carry out profiling on a large scale
☐ Process biometric or genetic data
☐ Combine, compare or match data from multiple sources
☐ Process personal data without providing a privacy notice directly to the individual
☐ Process personal data in a way that involves tracking individuals' online or offline location or behaviour
☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
☐ Process personal data that could result in a risk of physical harm in the event of a security breach

If you have ticked 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 dataprotection@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

[2] Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Step 2: Describe the processing

Details of the Personal Data
What type of personal data is being processed? Tick all that apply
☒ Education and training details ☒ Employment details ☐ Family, lifestyle and social circumstances ☐ Financial details ☐ Goods or services provided and related information ☐ Personal details issued as an identifier (e.g. NHS Number) ☒ Personal details, including any information that identifies the data subject and their personal characteristics
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)
Information currently collected for case load clients is: Name Address Postcode Mobile number Email Age and date of birth NI number Benefits Housing provider Housing tenure This is through referral forms and project sign up forms, action plans and contact notes.

What special category / sensitive data is being processed? Tick all that apply
☒ Physical or mental health
☐ Religious or philosophical beliefs
☐ Trade union membership
☐ Sexual orientation
☐ Criminal record
☐ Criminal proceedings
☒ Racial or ethnic origin
☐ Political opinions
☐ Biometric or Genetic data
☐ Gender status
☐ No special category / sensitive data
What is the nature of the data? Please provide further information
Data is used for: Eligibility Data collection for statistical analysis and reporting to commissioner. No specific data is shared with other departments within SCC or external partners. Personal data will not be shared with any other partner or department unless explicit permission is given to do so. Name, postcode, age, what they are attending for, any outcomes that can be reported on. Data is collected for statistical analysis only.

Does the project involve the use of social care data?
☐ Yes
☒ No
Does the project utilise existing and established IT systems, or require the use / procurement of a new system?
☒ Existing / established system
☐ New system

The nature of the processing
How will the data be collected? E.g. via form, system transfer, face to face etc.
Forms, Interviews, WhatsApp, Microsoft Teams, and Zoom Zoom and WhatsApp will not be used to store anything which could be considered personally identifiable information, regardless of encryption settings. SCC mobile telephones will be registered within Intune (Download Company Portal from the Device's application store) which at least gives us a measure of control (Specifically being able to disable them should they be lost or stolen)
How will the data be used?
The data collated will be using the data to ascertain suitable support and opportunities for the individual accessing the service. All data collated is collated from the individual to populate forms, all have the privacy statement and individuals are reminded that they have the right to withdraw their data should they wish to. Should a referral be made for additional support for the individual and the referral is to be made by SCC then explicit consent will be sought in order to do the referral. Where possible the SCC officer will support the individual to refer them selves if this is possible. Client files and contact notes are kept preventing an individual having to repeat their information multiple times. This is held securely on the SCC system. Where it is necessary to send forms for a digital signature, then all personal data is removed off the form for emailing purpose ensuring keeping personal data as safe as possible, and a password is supplied in a separate correspondence, this is done unless secure emails are able to be sent to the individual or professional. Due to the nature of the service, individuals understand that if there is a suitable course or opportunity that is suitable for them, they may be contacted about this. SCC officers and individuals generally meet weekly (digitally and face to face), and individuals have the opportunity and right to ask to not receive information, decline the service and be removed from a caseload. Individuals will only ever receive opportunities suitable for them and Employment or Training related. All data reported on for commissioners and funders is totally anonymised, using statistical data for reporting.
How will the data be stored?
SCC system in client files.
How will the data be deleted? E.g. Manually, via automated process etc.
Manually after 6 years

What is the source of the data? i.e. What is the flow of data into the Council?
Direct from the data subject via Forms, Interviews, WhatsApp, Teams, and Zoom
Will you be sharing data with anyone?
INFO: If yes, please provide details
Yes. The Council will usually seek to assist the data subjects make any referral themselves. However, in some circumstance the Council will make a referral on behalf of the data subject this will only be done with their specific informed consent using a consent form. The consent form is regularly updated and is used to record explicit consent where appropriate. Reporting is on outcomes only not individuals.
If so, how will the data be transferred?
If information is shared for referral purposes (the only reason for data sharing) then informed consent is sought, and information will be sent either by secured email, password protected or over the phone.
If the data is being shared, will this be governed by an agreement? e.g. contract, data sharing agreement, data processing agreement
Yes There is a client information sharing form, allowing individual names and details to be listed. This is a live document so can be updated by the client at any time. Information shared with employers is through clients, Employment Officers do not disclose or share information on behalf of the client. Referrals made by the Council on behalf of clients are made in line with the partner usual practice for receiving such referrals. The Council will only submit a referral on behalf of the data subject after it has explained to all relevant aspects of the partner organisations privacy policy (how the partner organisation will process their data, the purpose of the processing and who that data will be shared with).

Describe the scope of the processing
How often will the data be collected and used?
Monthly reporting (anonymized) and the records reviewed an updated after these meetings

How long will you keep it?
INFO: Please specify a time period, and the corresponding entry on the Council's Retention Schedule: https://staffinfo.southampton.gov.uk/information-governance/records-management/retention.aspx If unsure, contact the Senior Records Officer: records.management@southampton.gov.uk
6 years
How many individuals are affected?
One record for each interviewee – estimated total caseload 5,000 people over 3 years
What geographical area does it cover?
Southampton

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)
People wanting numeracy support and/or employment/skills support and accessing a range of projects funded through UKSPF and Multiply programmes
How much control will they have over their data? Will they be able to change it, access it, delete it etc.?
Service users need to agree to engage with the project and give their consent to participate, enabling SCC to collect, process, store and share their data for the purposes of project monitoring and reporting. All files are digitally stored as no paper files are kept. Data is retained for monitoring and reporting.
Would they reasonably expect the Council to use their data in this way?
INFO: Please provide details to support your answer
Yes, they will have engaged with the project and will have consented to the data being used in this way
Do they include children or other vulnerable groups?
INFO: If yes, please provide details
Not children, but some will be vulnerable adults

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? E.g. do other local authorities have a similar process in place?
INFO: If yes, please provide details
No. The processes described are standard ways of project delivery
Are there any current issues of public concern that should be considered?
INFO: If yes, please provide details
No

Describe the purposes of the processing
What do you want to achieve?
Support people's numeracy skills, employment and work skills, and to access a range of provision to improve residents' quality of life – sustainable travel, crime reduction, business support
What is the intended effect on individuals?
Improve the quality of life of residents
What are the benefits of the processing – for the Council, and more broadly?
INFO: Please confirm which of the Council's key outcomes this will support, and how
Outcome: ☒ Southampton has strong and sustainable economic growth ☐ Children and young people get a good start in life ☒ People in Southampton live safe, healthy, independent lives ☒ Southampton is an attractive modern city, where people are proud to live and work **How:** By supporting residents to be more economically self sufficient and to improve the quality of life where they live

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
Service users need to agree to engage with the project and give their consent to participate, enabling SCC to collect, process, store and share their data for the purposes of project monitoring and reporting. All files are digitally stored as no paper files are kept.
Who else do you need to involve, or have you already involved within the Council?
INFO: e.g. IT services, records management
(ITS consulted regarding use of Zoom and Whatsapp)
Do you need to ask your processors to assist?
INFO: Processors are third parties who will process the personal data on our behalf
No, there are no data processors in this project
Do you plan to consult information security experts, or any other experts?
INFO: Please provide details to support your answer

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures
What do you consider your lawful basis for processing to be? 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

Please provide further information to support this
INFO: For example, if the processing is necessary in order for the Council to perform a statutory function, detail the relevant legislation.
service users need to agree to engage with the project and give their consent to participate, enabling SCC and project partners to collect, process, store and share their data for the purposes of project monitoring and reporting. All files are digitally stored as no paper files are kept. Data is retained for monitoring and reporting.
Does the processing actually achieve your purpose?
INFO: Please provide details to support your answer
yes as it enables clients to be supported by SCC officers and anonymized data reported to central government
Is there another way to achieve the same outcome?
INFO: Please details to support your answer
no. People will need to provide confidential information in order to participate in the project
How will you prevent function creep?
INFO: Function creep is where data collected for one purpose is used for another purpose over time.
The data is not required for other purposes Only information necessary for the project will be collected It will be stored in such a way that only those involved in the project can access it
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.
Only need or want to collect minimal amounts of data agreed to by the data subject
What information will you give individuals about the processing?
All clients will be provide with a privacy statement which set out what information is being collected, the purpose of processing the data and how we will use it. Where the Council is sharing the data with a third party, the Council will advise the data subject of the organization they intend to share their data with, explain how that organization will use the data and ask the data subject if the consent to the data being shared.
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.
Information regarding why we want the data and how we will use it and the privacy statement will tell them how to access their personal data held by the Council
What measures do you take to ensure processors comply with the UK 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?
yes The project will provide the data subjects with a privacy statement detailing how their data will be used and how to exercise their data rights. Where necessary the privacy statement will be explained further to the data subject. All information held and processed by the Council in relation to this project will be compatible with relevant Council policies. Data will only be share with third party organisations with the expressed and informed consent of the data subject expressed consent of the data subject
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

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 dataprotection@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. There is a risk of breaching the 6th data protection principle (personal data shall be processed in a manner that ensures appropriate security of the personal data). Whilst Zoom and WhatsApp offers a level of security, the Council's Head of IT is unhappy to provide assurances that this level is adequate, when there is a supported platform (Microsoft Teams) that will provide an appropriate level of security. The project team do not intend to "store" any personal data on Zoom or WhatsApp. However, it is likely that any communication via Zoom or WhatsApp is likely involve personal data (Even, as simply as Phone number X called Phone number Y). Zoom and WhatsApp are likely to store at least some personal data. A breach of the 6th data protection principle could lead to a fine of up to € 20million, and a data subject has the right to compensation for and damage / distress caused by a breach, which could be unlimited. The overall risk has been assessed as Low, due to the likelihood of a breach occurring, and the sensitivity of the information that a third party would have access to, should a breach occur.			
2. There is a risk of breaching Article 28 of the UK GDPR, which states that we must have a contract / legal agreement in place with our data processors, and that the contract must contain certain clauses on data protection. It is unlikely getting such a contract in place with Zoom or WhatsApp will not be possible in relation to this project.			

The clauses set out in Article 28 offer the Council protection should a security breach occur, where the fault lies with the processor and not with the Council. The extent on whether Zoom and WhatsApp are our data processor does depend on the cloud storage aspect, but there is still an argument that they are our data processor without this; we still provide them with some personal data in the form of contact information and names. A breach of Article 28 could lead to a fine of up to €10million, and a data subject has the right to compensation for and damage / distress caused by a breach, which could be unlimited. The overall risk has been assessed as Low, due to the likelihood of a breach occurring, and the sensitivity of the information that a third party would have access to, should a breach occur.			
3. Where the data controller relies on consent, there is a risk that; • The data subject has not consented to all aspects of processing • The consent is not informed consent • The consent is freely given • It is not as easy to withdraw consent as it is to give it Where the conditions for consent set out in the UK GDPR Article 7 are not met, there is no consent and the Council cannot rely on consent as the legal basis for processing data. If there is no legal basis for processing the data, the processing is unlawful. Therefore, there is a risk that the 1st Data Protection Principle will be breached (personal data must be processed lawfully, fairly, and in a transparent manner). A breach of the 1st Data Protection Principle could lead to a fine of up to €20million, and a data subject has the right to compensation for any damage / distress caused by a breach, which could be unlimited.			

The overall risk has been assessed as low because the data will be processed to benefit the data subject or for statistical purposes that have no direct impact on the data subject.			

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

Condition(s) for Processing
Personal Data
☐ 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
Further Information
I have highlighted some measure within my comments below to ensure that the conditions of consent are met.
Special Categories of Personal Data
☐ The data subject has given explicit consent ☐ The 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 ☐ The processing is necessary for reasons of substantial public interest ☐ The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems ☐ The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ☐ No special category data being processed
Further Information

Data Protection Act 2018 Schedule 1 Condition
Further Information

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.	In order to eliminate this risk, consideration should be given to using the supported platform, Microsoft Teams. Should this not be considered viable, this risk will need to be accepted by the Information Asset Owner.		
2.	In order to eliminate this risk, consideration should be given to using the supported platform, Microsoft Teams. Should this not be considered viable, this risk will need to be accepted by the Information Asset Owner.		
3.	The project team to ensure that; • the data subject understands how their data will be processed • when dealing with special category data, the data subject specifically understands what is happening with that data and they give explicit consent for that processing to happen • the data subject gives specific consent to each type of data processing. • The data subject understand that there is no benefit to giving consent or no cost to withholding consent except those that directly flow from the processing For example giving consent is not a condition of participation in the project. • The data subject understands they can withdraw their consent at any time, and they know how to do this. • There is an effective process for immediately processing a withdrawal of consent		

	• To ensure that where data is used for statistic purposes that data is anonymised at the earliest opportunity. Where data is held unable to be anonymised that processing of that data can be ceased immediately upon the withdrawal of consent.		
Comments from the Data Protection Officer			
Comments from the Senior Records Officer			
Comments from the Head of IT			

Step 8: Sign off

Item	Date	Notes
DPO reviewed DPIA and provided advice on:		
Senior Records Officer reviewed DPIA on:		
Head of IT reviewed DPIA on:		
Measures approved by Project Lead on:		
Comments from Project Lead:		
Residual risks approved by Information Asset Owner / Administrator on:		
Comments from IAO / IAA:		
Project approved by Caldicott Guardian (CG) on:		
Comments from CG:		
Residual high risks approved by the Senior Information Risk Owner (SIRO) on:		
Comments from SIRO:		

Step 9: Review

Item	Date	Comments
DPO reviewed DPIA on:		

Date of next review:	