DATA PROTECTION IMPACT ASSESSMENT - INTEGRATED WELLBEING SERVICE (IWS) V1.0

Reference number: DPIA-(reference number to be determined)

Author: Vicky Lewis
Email: Vicky.lewis@nottinghamcity.gov.uk

DATA PROTECTION IMPACT ASSESSMENT

When to complete this template:

Start to fill out the template at the beginning of any major project involving the use of personal data, or, where you are making a significant change to an existing process that affects personal data. Please ensure you update your project plan with the outcomes of the DPIA.

Table of Contents

1. Document Control

1. Control Details

Author of DPIA:	Vicky Lewis, Public Health Commissioning officer
Owner of project:	Matt Corder, Public Health Principal
Contact details of Author:	Vicky.lewis@nottingham.gov.uk

2. Document Amendment Record

Issue	Amendment Detail	Author	Date	Approved
1.0	DPIA created	Vicky Lewis	15/05/23	

3. Contributors/Reviewers

Name	Position	Date
Matt Corder	Public Health Principal	

4. Glossary of Terms

Term	Description
Please insert any abbreviations you wish to use:	

Author: Vicky Lewis
Email: jeremy.lyncook@nottinghamcity.gov.uk

2. Screening Questions

1. Does the project involve personal data? **Yes**	**If 'Yes', answer the questions below. If 'No', you do not need to complete a DPIA but make sure you record the decision in the project documentation.**
2. Does the processing involve any of the following data: medical data, ethnicity, criminal data, biometric data, genetic data, and any other special/ sensitive data?	**Yes**
2. Does the processing involve any systematic or extensive profiling?	**No**
3. Does the project involve processing children's data or other vulnerable citizen's data?	**Yes**
4. Does the processing involve decisions about an individual's access to a product, service, opportunity, or benefit that is based on any evaluation, scoring, or automated decision-making process?	**Yes**
5. Does the processing involve the use of innovative or new technology or the novel application of existing technologies?	**No**
6. Does this project involve processing personal data that could result in a risk of physical harm in the event of a security breach?	**No**
7. Does the processing combine, compare, or match data from multiple sources?	**No**
8. Does the project involve processing personal data without providing a privacy notice?	**No**
9. Does this project process data in a way that tracks online or offline location or behaviour?	**No**
10. Will the project involve using data in a way it has not been used before?	**No**
11. Does the project involve processing personal data on a larger scale?	**Yes**
12. Will the project involve processing data that might prevent the Data Subject from exercising a right or using a service or entering a contract?	**No**

If you answered 'Yes' to any <u>two</u> of the questions above, proceed to Question 3 below. If not seek advice from the DPO as you may not need to carry out a DPIA.	

Project Title: Integrated Wellbeing Service (IWS) - 2024 onwards

Team: Public Health

Directorate: Peoples

DPIA Reference number: *(This will be allocated by the Information Compliance Team or the DPO and must be quoted in all correspondence)*

Has Consultation been carried out?

To help the Council make sure that proposals meet the current needs and demands of the population, we have asked service users, strategic partners, and local services for their views. We were also keen to hear the views of the wider public, those who may wish to access health improvement services directly or support services in the future.

The feedback has helped the strategic commissioning process to:

- Understand how services can be structured to best meet the needs of current and future service users across Nottingham
- Achieve the best health outcomes possible with the funding available, and to understand how these outcomes can be met whilst ensuring Best Value
- Identify the key issues around services, to agree what the priorities in Nottingham should be for the coming years
- Gain a deeper understanding of how to best utilise and improve pathways and links between services.

Engagement and consultation on the Council's proposals has taken place in two stages: stage 1 to l inform the development of an Integrated Wellbeing Service model and stage 2 will refine and finalise an Integrated Wellbeing Service model.

Engagement and consultation activities to date include:

1) A public engagement survey collecting views and local need from citizens and partner organisations

- ongoing - survey is live for an 8-week period (from 31st March 2023 to 30th May 2023)
- Available in digital format (via Nottingham Engage Hub) and hard-printed copies
- Survey link has been promoted via Nottingham City Council's social media platforms
- Survey link has been shared with internal Public Health team and key stakeholders such as Nottingham's Community and Voluntary Sector, Nottingham and Nottinghamshire Health watch, NHS, ICB, SSBC and across targeted groups such as Health Improvement Steering Group, Reducing Harm Group and various Severe Multiple Disadvantaged groups

2) Soft market engagement with providers

- Online event 17th April 2023

- Approximately 60 service providers were present (a mix of local and national service providers, partners, and voluntary, community & social enterprise)
- Provided an opportunity to develop connections amongst service providers (including existing service providers)
- Contact details for all those registered were shared to facilitate and encourage dialog between service providers
- A follow-up online survey was shared with those registered onto the event and 20 responses were submitted. Questions related to the opinions around proposed scope, potential barriers, contract length, finance, appetite to bid and any further comments
- Responses were automatically anonymised to encourage honest feedback on the Council's IWS proposals
- Dialogue will enable officers to incorporate provider proposals and innovations within the final Service Specification

<u>3) Input regarding service design from key stakeholders</u>

- Conversations with ICB, University of Nottingham, Nottingham CVS, Nottingham City Council, Nottingham University Hospitals
- Discussed opportunities to co-commission
- Ongoing conversations

1. DDM attached?	**Yes** **Commissioning and Procurement Executive Committee (CPEC) – 30th May 2023**
2. Written evidence of consultation carried out attached?	**Yes**
3. Project specification/ summary attached?	**Yes**
4. Any existing or previous contract / SLA / processing agreement attached?	**No – New service**
5. Any relevant tendering documents attached?	**No**
6. Any other relevant documentation attached?	**No**

3. Project - impact on individual's privacy

Issue	Questions	Examples	Yes/No	Initial comments on issue & privacy impacts
Purpose and means		Profiling, data analytics, Marketing. Note: The GDPR requires a DPIA to be carried out where there is systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling, and on which decisions about individuals are based.		
	Please give a summary of what your project is about (*you can also attach or embed documents for example a project proposal*).			Nottingham City Council currently commissions several separate contracts to individual service providers to deliver health improvement interventions across Nottingham. From April 2024, the Council intends to amalgamate a range of health improvement interventions into one service model, referred to as an Integrated Wellbeing Service (IWS). The Council will seek to commission a prime provider model, which will be responsible for delivering the service functions in an innovative, dynamic, and flexible manner across Nottingham, ensuring Best Value with the following objectives: • Maintaining and improving the health of Nottingham City citizens • Preventing future ill-health and its negative impacts on the local population • Reducing future and existing pressures on local health and care services • Putting the service user at the centre of provision, in-line with the personalisation agenda. In a prime provider model, the council contracts with a single organisation (or consortium) which then sub-contracts individual providers to deliver the required programmes and interventions within the service specification they can also deliver elements of the service themselves. The council retains overall accountability for the commissioned service, while the Service Provider holds each of the sub-contractors to account individually. The Service Provider takes responsibility for designing a delivery model and subsequent pathways that will most effectively meet the terms of the contract.

			It uses the terms of the sub-contracts to stimulate and incentivise the necessary behaviours and performance it wishes to see across other providers.
	Aims of project Explain broadly what the project aims to achieve and what types of processing it involves.		The proposed Integrated Wellbeing Service will provide a single-entry point to health and wellbeing support for residents wishing to address lifestyle and behavioural factors (such as smoking or weight management) whilst considering support and signposting around the wider determinants such as emotional wellbeing and other factors that might be negatively impacting their health. The service will focus on taking a life course approach to prevention of ill health, valuing the health and wellbeing of both current and future generations. Addressing the wider determinants of health will help improve overall population health, individual wellbeing, and the conditions which people are born, live, learn and work. This will follow a sensitive and responsive local needs approach by working 'with' rather than 'in' communities. To that extent, the service will be place and asset-based i.e. tailored to local needs. The behaviour change service will be required to link with and compliment the wider offers in the community and provide additional resources to further develop healthy communities and environments locally.
	Describe the nature of the processing How will you collect store and delete data? Will you be sharing with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved? Who will have access to the project personal data, how is access controlled and monitored		The Service Provider will deliver the service on behalf of the Council, as commissioner. As part of service provision, it will be necessary for the provider to collect and store data relating to citizens. The Council and the Service Provider are both Data Controllers and Data Subjects shall be the citizens using the service, in line with UK General Data Protection Regulations (GDPR) and Data Protection Act 2018. In collecting Personal and Special Category Data, the Service Provider will be responsible for: • Maintaining accurate records of Service User consent • Informing Service Users that consent can be withdrawn, prior to consent being give, and how to go about it

	and reliability of staff assessed? Will data be separated from other data within the system?		• Responding to: - subject access request (SAR) (as per Article 15 of the GDPR) - request to block, rectify or erase personal data relating to data subjects - request for disclosure from a 3rd party, where compliance with a request is required or purported to be required by law Referrals into the service will be made directly to the Service Provider by: • Health professionals • Support services • Self-referral A process will be agreed against the Service Provider and the Council, as commissioner but ultimately, health professionals and support services will use a referral form to record citizen data which will be shared with the Service Provider. The Service Provider will use the information contained on the referral form to follow up and discuss with the citizen their needs and the outcomes they wish to achieve from receiving the service. The Service Provider will keep and store the referral information. The referral form is saved to the Service User's record on a robust IT/data management system. The Service Provider may decide that the citizens would benefit from additional support from within their organisation or from an external organisation. This would involve an onward referral from the Service Provider to the external organisation/provider. The Council requires the Service Provider to share the outcomes of the referral with Commissioners so that the impact of the service can be monitored, and improvement activities can be put in place if necessary. This will involve the Service Provider sharing anonymised referral information and outcome measurement information (this is a process which determines

			whether desired outcomes agreed at the referral stage have been achieved and it would be a discussion that takes place between the citizen and the Service Provider). To further determine what the wider outcomes of the service are, the Council may use the referral data and outcome data to link to wider system outcomes such as whether a hospital admission occurred while the Service User was being supported. The Service Provider will keep and store the Service User's information on a robust IT/data management system to identify whether there were any linked outcomes for the Service User after a referral to the service was made. The parties that will have access to the project personal data include: • The referral organisation/worker who made the original referral • The Service Provider • The Council, as commissioners of the service • The Service User The Service Provider will be responsible for ensuring there is a robust IT/data management system to hold and process data for each individual Data Subject and kept in accordance with the requirements of Article 32 of the GDPR. The Service Provider shall collect, record, and store the Data Subject's relevant information, in a secure manner, which protects confidentiality. The Service Provider must have procedures in place to report misuse, loss, destruction, damage, or unauthorised access, suspected or otherwise, of information. The Service Provider shall store the Data Subject's collected data until after the stipulated number of years after the end of the Contract Period (or as long a period as may be agreed between the Parties). The Service Provider shall destroy the Data Subject's data either at the end of the retention period or at the request of the applicant, whichever is the sooner.

			The Service Provider shall destroy the data it holds in relation to this specific service at the end of the above period in accordance with Data Protection legislation. A record of the work carried out with the Data Subject shall be shared with the Data Subject in the event of a subject access request, by providing a printed record of the applicant's system data. The Service Provider must provide clear information to Service Users accessing the Service on what data will be collected, by whom, the purpose, as well as how it will be collected, stored and destroyed, in line with the required retention period. The Service Provider must not transfer any personal data outside the European Union or European Economic Area without the express permission of the commissioning authorities. The Service Provider shall share statistical data with the Council for the purposes of monitoring of performance against the contract and informing future commissioning. The Service Provider must develop a Privacy Notice as part of the Implementation Period and made easily available to Service Users (including on their website and in a written format) from the contract start date. The Council will work with the Service Provider to develop an Information Sharing Agreement during the Implementation Period. A Third-Party Security Questionnaire will be completed by the Service Provider as part of the Invitation to Tender, this will identify the organisations Information Governance maturity for example the technical and organisational measures in place to protect the data being collected and processed as part of the Service. The Service Provider will ensure that any Sub-contractors/Partners that process any personal data enters into a written agreement which gives effect to the same terms as set out in the Agreement and are subject to the same data protection obligations.

			All organisations that have access to NHS patient data and systems must use the Data security and protection toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. The Service Provider shall ensure staff with authorised access to any Personal Data are aware of their obligations under the Data Protection Legislation to safeguard that information. The Service Provider's employees should have appropriate information governance training to enable them to undertake their duties confidently, efficiently, and lawfully. The Service Provider and its employees must be fully compliant with the UK's GDPR regulations.	
	Privacy Implications Can you think of any privacy implications in relation to this project? How will you ensure that use of personal data in the project is limited to these (or "compatible") purposes?		No	Citizen data/information is being shared with the Service Provider may contain sensitive or personal medical information. The referral information will only be accessed by the Service Provider for the purposes of delivering the service. Information contained within the referral form will be specifically related to the citizen and their needs to enable the service provider to create a support plan and to ensure an appropriate volunteer is allocated to deliver the plan.
	New Purpose Does your project involve a new purpose for which personal data are used?		No	Improved referral pathway - referrals into the service will be made directly to the Service Provider by: • Health professionals • Support services • Self-referral
	Consultation 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. Who else		Yes	I will be seeking the views of the Service Provider and key stakeholders (such as hospitals, GP's etc.) who will be able to provide advice about what citizen information needs to be included within the referral form.

	do you need to involve in NCC? Do you plan to consult Information security experts, or any other experts?			I will be consulting with a member of the Council's Information Compliance team.
Individuals (data subjects)	Will the project:	Expanding customer base; Technology which must be used by individuals; Hidden or complex uses of data; Children's data		
	Affect an increased number, or a new group, or demographic of individuals (to existing activities)?		No	
	Involve a change to the way in which individuals may be contacted, or are given access to services or data? Are there any areas of public concern that you should factor in?		Yes	Improved referral pathway - referrals into the service will be made directly to the Service Provider by: • Health professionals • Support services • Self-referral
	Affect particularly vulnerable individuals, including children?		Yes	The service may be accessed by vulnerable service users with a range of physical or mental health/wellbeing issues.
	Give rise to a risk that individuals may not know or understand how their data are being used?		No	The Service Provider must provide clear information to Service Users accessing the Service on what data will be collected, by whom, the purpose, as well as how it will be collected, stored and destroyed, in line with the required retention period.
Parties	Does the project involve:	Outsources service providers; Business partners; Joint ventures		
	The disclosure of personal data to new parties?		Yes	The Service Provider may be required to make onward referrals, sharing the referral data with external agencies who can provide specific support for the citizen. E.g. local hospitals, GP's or other community or voluntary sector organisations or charities.

	The involvement of sharing of personal data between multiple parties?		Yes	It could involve the sharing of data between multiple parties – as per the answer to the above question.
Data categories	Does the project involve:	Special personal data; Biometrics or genetic data; Criminal offences; Financial data; Health or social data; Data analytics: Note: the GDPR requires a DPIA to be carried out where there is processing on a large scale of special categories of data or of data relating to criminal convictions and offences		
	The collection, creation or use of new types of data?		Yes	It will involve collection of information from the citizen to determine whether the service has helped them to achieve personal goals and outcomes. This will be recorded on a separate form to the referral form.
	Use of any special or privacy-intrusive data involved? • Political opinions • Religious beliefs or philosophical beliefs • Trade union membership • Genetic data • Biometric data • Sexual life • Prosecutions • Medical data • Criminal data (Criminal data processing, i.e. criminal convictions, etc. also has special safeguards under Article 10)		Yes	Some medical data/information relating to specific medical conditions which would need to be considered by the Service Provider in order to assess the individual and deliver support effectively e.g. if the Service User had spent recent time in hospital following a fall and was recovering from a broken bone then mobility may be reduced and the support provided would need to be appropriate for the citizens recovery. Nottingham City Council is committed to equality of opportunity. Equalities monitoring allows us to ensure that everybody is receiving the services that they are entitled to. Although some of this data is not mandatory for the Service User to provide to Service provider, demographic information (such as ethnicity, gender, religious beliefs and sexual orientation), will be requested to enable the Council to monitor equal opportunities, with the ultimate aim to improve access to services.

	New identifiers, or consolidation or matching of data from multiple sources? (For example a unique reference number allocated by a new management system)		Yes	The only identifier will be the Service User's unique reference number (if they have one) for the Service Provider to review the performance of the service to determine whether outcomes for the citizen were achieved.
Technology	New solutions:	Locator or surveillance technologies; Facial recognition; Note: the GDPR requires a DPIA to be carried out in particular where new technologies are involved (and if a high risk is likely)		
	Does the project involve new technology that may be privacy-intrusive?		No	

Data quality, scale and storage	Data:	New data		
	Does the project involve changes to data quality, format, security or retention? What are the benefits of the processing? i.e. will the new system have automatic retention features? Will the system keep the information in a safer format etc.?		No	
	Does the project involve processing data on an unusually large scale?		No	
Monitoring, personal intrusion	Monitoring:	Surveillance; GPS tracking; Bodily testing; Searching; Note: the GDPR requires a DPIA to be carried out where the project involves systematic monitoring of a publicly accessible area on a large scale		
	Does the project involve monitoring or tracking of individuals or activities in which individuals are involved?		Yes	Yes, the methodology requires regular discussion between Service Provider and Service User to track the Service User's progress in relation to agreed personal goals or outcomes. The Service Provider will share aggregated service data with the Council, as commissioner.
	Does the project involve any intrusion of the person?		No	
Data transfers	Transfers	Transfers outside the EEA		
	Does the project involve the transfer of data to or activities within a country that has inadequate or significantly different data protection and privacy laws?		No	

4. Legal Framework and Governance – Compliance

Ref.	Question	Response	**Further action required** (and ref. to risk register as appropriate)
1. Applicable laws and regulation			
1.1	Which data protection laws, or laws which impact data protection and privacy, will be applicable to the project?	• General Data Protection Regulation 2016/679 • UK General Data Protection Regulation • Data Protection Act 2018 • Human Rights Act 1998	
1.2	Are there any sector-specific or other regulatory requirements or codes of practice, which should be followed?	• The Care Act 2014	
2. Organisation's policies			
2.1	Is the project in compliance with the organisation`s information management policies and procedures (including data protection, information security, electronic communications)?	Yes	

2.2	Which policy requirements will need to be followed throughout design and implementation of the project?	Data Protection Policy Information Security Policy Records Management Policy	
2.3	Are any changes/updates required to the organisation`s policies and procedures to take into account the project? **Note: new requirements for *"Accountability"* under the GDPR, including record-keeping, DPOs and policies**	No	
3. Training and roles			
3.1	Will any additional training be needed for staff in relation to privacy and data protection matters arising from the project?	Yes	The Service Provider shall ensure staff with authorised access to any Personal Data are aware of their obligations under the Data Protection Legislation to safeguard that information. The Service Provider's employees should have appropriate information governance training to enable them to undertake their duties confidently, efficiently, and lawfully. The Service Provider and its employees must be fully compliant with the UK's GDPR regulations.

5. Personal Data Processing Compliance

Ref.	Question	Response	Further action required (and ref. to risk register as appropriate)
1.	**Personal Data Processing**		
1.1	Which aspects of the project will involve the processing of personal data relating to living individuals?	The collection of personal data will take place during the referral process. Referrals into the service will be made directly to the Service Provider by: • Health professionals • Support services • Self-referral The processing of personal data will take place when the Service Provider is assessing the needs of the citizen and creating the personalised support plan or the onward referral. The outcomes of the support (including the outcomes for the Service User) will be recorded by the Service Provider and it is requested that this is then shared with Nottingham City Council, as commissioner.	
1.2	Who is/are the data controller(s) in relation to such processing activities?	• Service Provider, externally commissioned by Nottingham City Council • Nottingham City Council, as commissioner	
1.3	Who is/are the data processor in relations to such processing activities?	• Service Provider, externally commissioned by Nottingham City Council	
2.	**Fair and Lawful processing - GDPR Articles 5(1)(a), 6, 9, 12, 13**		

2.1	Which fair processing conditions are you relying on? GDPR: Article 6(1) (legal basis for processing) and, for sensitive personal data, Article 9(2).	6(1). **Choose at least one of the following for personal data**, **usually (e)**-(Cross out the rest) ~~a) Consent~~ ~~b) Performance of contract~~ ~~c) Legal obligation~~ ~~d) Vital interests~~ **e) Public interest / exercise of Authority** 9(2) Choose at least 1 for special data- usually g (cross the rest out) ~~a) Explicit consent~~ ~~b) Employment / social security / social protection obligations~~ ~~c) Vital interests~~ ~~d) Non-profit bodies~~ ~~e) Processing made public by data subject~~ ~~f) Legal claims~~ ~~g) Substantial public interest~~ h) Health, social care, medicine I) Public interest for public health ~~j) Archiving, statistics, historical research~~ **For any criminal Data** Comply with Article 10 **if it meets a condition in Part 1, 2 or 3 of Schedule 1.** • ~~Employment, social security, and social protection~~ • ~~Health and social care purposes~~ • Public health • ~~Research~~ Substantial public interest: • Statutory and government purposes • Equality of opportunity and treatment	

		• ~~Racial and ethnic diversity at senior levels of organisations~~ • ~~Preventing or detecting Unlawful Acts~~ • ~~Protecting the public against dishonesty etc~~ • ~~Regulatory requirements relating to unlawful acts and dishonesty etc~~ • ~~Journalism etc in connection with unlawful acts and dishonesty etc~~ • ~~Preventing fraud~~ • ~~Suspicion of terrorist financing or money laundering~~ • ~~Counselling~~ • ~~Safeguarding of children and of individuals at risk~~ • ~~Safeguarding of economic well-being of certain individuals~~ • ~~Insurance~~ • ~~Occupational pensions~~ • ~~Political parties processing~~ • ~~Disclosure to elected representatives~~ • ~~Informing elected representatives about prisoners~~ Additional Conditions • ~~Consent~~ • ~~Vital interests~~ • ~~Personal data in the public domain~~ • ~~Legal claims~~ • ~~Judicial Acts~~	
Note: different conditions may be relied upon for different elements of the project and different processing activities. Also, the scope of special category data is wider under the GDPR, and in particular includes genetics & biometric data, and sexual orientation.			

2.2	How will any consents be evidenced and how will requests to withdraw consent be managed?		
Note: new requirements for obtaining and managing consents within the GDPR.			
2.3	Is the data processing under the project covered by fair processing information already provided to individuals or is a new communication needed (see also data subject rights below)?	Yes	The Service Provider must develop a Privacy Notice as part of the Implementation Period and made easily available to Service Users (including on their website and in a written format) from the contract start date. The Council will work with the Service Provider to develop an Information Sharing Agreement during the Implementation Period.
Note: more extensive information required under the GDPR than under current law, and new requirements on how such information is provided. Also a general principle of "*transparency*". It is important to assess necessity and Proportionality			
2.4	If data is collected from a third party, are any data protection arrangements made with such third party?	Yes	A Third-Party Security Questionnaire will be completed by the Service Provider as part of the Invitation to Tender, this will identify the organisations Information Governance maturity for example the technical and organisational measures in place to protect the data being collected and processed as part of the Service. The Service Provider will ensure that any Sub-contractors/Partners that process any personal data enters into a written agreement which gives effect to the same terms as set out in the Agreement and are subject to the same data protection obligations.

			All organisations that have access to NHS patient data and systems must use the Data security and protection toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.
2.5	Is there a risk of anyone being misled or deceived?	No	
2.6	Is the processing "fair" and proportionate to the need's and aims of the projects?	Yes	
2.7	Are these purposes clear in privacy notices to individuals? (see above)	Yes	The Service Provider must develop a Privacy Notice as part of the Implementation Period and made easily available to Service Users (including on their website and in a written format) from the contract start date. The Council will work with the Service Provider to develop an Information Sharing Agreement during the Implementation Period.

3. Adequate, relevant and not excessive, data minimisation - GDPR Article 5(1)(c)			
3.1	Is each category relevant and necessary for the project? Is there any data you could not use and still achieve the same goals?	Yes	
Note: GDPR requires data to be "limited to what is necessary" for the purposes (as well as adequate and relevant).			
3.2	Is/can data be anonymised (or pseudonymised) for the project?	Partly	The service provider needs to be able to make direct contact with the Service User and personal information will be a requirement of the referral process.

			As commissioner, the Council does not require the same level of personal data from the Service Provider to monitor outcome targets and receive case studies etc. Therefore, the Council will only request the required level of detail of Service Users (likely the monitoring data will be anonymised by the Service Provider when sent to the Council) as part of the quarterly monitoring meetings with the Service Provider.
4. Accurate and up to date - GDPR Article 5(1)(d)			
4.1	What steps will be taken to ensure accurate data is recorded and used?		The Service Provider will be responsible for ensuring there is a robust IT/data management system to hold and process data for each individual Data Subject and kept in accordance with the requirements of Article 32 of the GDPR. The Service Provider shall collect, record, and store the Data Subject's relevant information, in a secure manner, which protects confidentiality.
For example: checks when receiving/sending information from/to third parties, or transcribing information from oral conversations or handwritten documents, any automatic checks on information not meeting certain criteria.			
4.2	Will regular checks be made to ensure project data is up to date?	Yes	Quarterly monitoring meetings will be held between the Council and Service Provider, as a minimum.
5. Data retention - GDPR Article 5(1)(e)			
5.1	How long will personal data included within the project be retained?		The Service Provider shall store the Data Subject's collected data until after the stipulated number of years after the end of

			the Contract Period (or as long a period as may be agreed between the Parties). The Service Provider shall destroy the Data Subject's data either at the end of the retention period or at the request of the applicant, whichever is the sooner. The Service Provider shall destroy the data it holds in relation to this specific service at the end of the above period in accordance with Data Protection legislation. A record of the work carried out with the Data Subject shall be shared with the Data Subject in the event of a subject access request, by providing a printed record of the applicant's system data.
5.2	How will redundant data be identified and deleted in practice? Consider paper records, electronic records, equipment?		The Service Provider must have procedures in place to report misuse, loss, destruction, damage, or unauthorised access, suspected or otherwise, of information.
5.3	Can redundant data be easily separated from data which still need to be retained?		When the Service Provider is separating redundant data from data which needs to be retained, they will need to ensure paper records as well as online records are considered as part of the separation process.
6. Data subject rights - GDPR Articles 12 to 22			
6.1	Who are the relevant data subjects?		Data Subjects shall be the citizens using the service.

6.2	Will data within the project be within the scope of the organisation`s subject access request procedure?	Yes	Some information will be kept by the Service Provider only and therefore a request should be made to them as Data Controllers directly.
6.3	Are there any limitations on access by data subjects?	No	
6.4	Is any data processing under the project likely to cause damage or distress to data subjects? How are notifications from individuals in relation to damage and distress managed?	No	
6.5	Does the project involve any direct marketing to individuals? How are requests from data subjects not to receive direct marketing managed?	No	
6.6	Does the project involve any automated decision making? How are notifications from data subjects in relation to such decisions managed?	No	
6.7	How will other rights of data subjects be addressed? How will security breaches be managed?		These rights will be processed by the Information Compliance Team at Nottingham City Council. All breaches will be dealt with by the Information Compliance team and the Data Protection Officer.

7. Data Security - GDPR Articles 5(1)(f), 32

For example:

- **Technology**: encryption, anti-virus, network controls, backups, DR, intrusion detection;
- **Physical**: building security, clear desks, lock-leads, locked cabinets, confidential waste;
  Organisational: protocols on use of technology, asset registers, training for staff, pseudonymisation, regular testing of security measures.

Describe the source of risk and nature of potential impact on the individuals. Include associated compliance and corporate risks as necessary -What security measures and controls will be	**Likelihood of harm**	**Severity of harm**	**Overall Risk**

incorporated into or applied to the project to protect personal data? Consider those that apply throughout the organisation and those which will be specific to the project. N.B Measures that are appropriate to the nature of the data and the harm which may result from a security breach	Remote, Possible or Probable	Minimal, Significant or Severe	Low, Medium or High
Technology: encryption, anti-virus, network controls, backups, DR, intrusion detection	Possible	Significant	Low
Incorrect data management	Possible	Significant	Low
Service User is unhappy to share personal data and referral information	Possible	Minimal	Medium
Service User information is shared inappropriately by the Service Provider	Possible	Minimal	Low

Identify measures to Reduce Risk- Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk that you have identified

Risk	Options to reduce or eliminate risk	**Effect on risk** Eliminated/ Reduced or Accepted	**Residual risk** Low/Medium/High	**Measures approved** Yes/No
Technology: encryption, anti-virus, network controls, backups, DR, intrusion detection	The Service Provider will be responsible for ensuring there is a robust IT/data management system to hold and process data for each individual Data Subject and kept in accordance with the requirements of Article 32 of the GDPR. The Service Provider shall	Risk reduced and accepted	Low	

	collect, record, and store the Data Subject's relevant information, in a secure manner, which protects confidentiality. Details will be included within the Service Specification.			
Incorrect data management	The Service Provider must have procedures in place to report misuse, loss, destruction, damage, or unauthorised access, suspected or otherwise, of information. The Service Provider will use minimal paper records and pseudonymised where possible. Details will be included within the Service Specification.	Risk reduced and accepted	Low	
Service User is unhappy to share personal data and referral information	The Service Provider must provide clear information to Service Users accessing the Service on what data	Risk reduced and accepted	Low	

	will be collected, by whom, the purpose, as well as how it will be collected, stored and destroyed, in line with the required retention period. Service Provider employees will be appropriately trained/ experienced in discussing support needs and support options with Service Users and this would normally include discussing referrals and gaining consent to complete referral forms on behalf of Service Users. Details will be included within the Service Specification.			
Service User information is shared inappropriately by the Service Provider to other organisations/stakeholders	The Service Provider will be aware of referral pathways and all employees will be trained appropriately for handling personal data.	Risk reduced and accepted	Low	

	Details will be included within the Service Specification.			
8. Data processors - GDPR Article 28 & direct obligations in other articles				
8.1	Are any data processors involved in the project?	No		
8.2	What security guarantees do you have?	N/A		
For example: specific security standards or measures, reputation and reviews				
8.3	Please attach the processing agreement			
For example: security terms, requirements to act on your instructions, regular audits or other ongoing guarantees Note: new requirements for the terms of contracts under the GDPR (much more detailed than current law).				
8.4	How will the contract and actions of the data processor be monitored and enforced?		Power to audit under the processing agreement	
8.5	How will direct obligations of data processors be managed?		Under the processing agreement	
Note: New direct obligations for processors under the GDPR, including security, data protection officer, record-keeping, international data transfers.				
For example: fair & lawful, lawful purpose, data subject aware, security, relevance.				
9. International data transfers - GDPR Articles 44 to 50				
9.1	Does the project involve any transfers of personal data outside the European Union or European Economic Area?	No	The Service Provider must not transfer any personal data outside the European Union or European Economic Area without the express permission of the commissioning authorities.	
9.2	What steps are taken to overcome the restrictions?	N/A		
For example: Safe Country, contractual measures, binding corporate rules, internal assessments of adequacy Note: GDPR has similar methods to overcome restrictions as under current law, but there are differences to the detail and less scope for an "own assessment" of adequacy.				

10. Exemptions			
10.1	Will any exemptions for specific types of processing and/or specific DP requirements be relied upon for the project?	No	
For example: crime prevention, national security, regulatory purposes Note: Exemptions under the GDPR to be assessed separately, and may be defined within additional EU or UK laws.			

6. Sign off and record outcomes

Item	Name	Date
Measures approved by: (project owner) This must be signed before the DP can sign off on the DPIA.		
Residual risks approved by: (If accepting any residual high risk, consult the ICO before going ahead)		
DPO advice provided: (DPO should advise on compliance, measures and whether processing can proceed)		
Summary of DPO advice:		
DPO advice accepted or overruled by		If overruled, you must explain your reasons
Comments:		
IT Security Officer: Where there are IT security issues		
IT Officer comments:		
SIRO Sign off: (For major projects)		
Consultation responses reviewed by:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA