	A	B	C	D	E
1	**Risk**	**Risk to individual or SBC**	**Mitigation**	**Consideration/Evaluation**	
2	System data is accessed by unauthorised persons and used or shared inappropriately	Contravention of services users' rights in relation to privacy, or loss, damage, misuse or abuse of their personal information	Access to the system will be limited to only those with the need to know. The use of the system will be managed locally through relevant training and guidance. Will need organisational measures to ensure only relevant staff access the data.	The benefits of storing the information greatly outweigh the privacy risk with the appropriate mitigations in place.	
3	Third parties use or share data inappropriately either due to inappropriate actions or insufficient technical and organisational measures.	Contravention of clients' rights in relation to privacy, or loss, damage, misuse or abuse of their personal information	Need a GDPR compliant legal agreement with all 3rd parties; details to be determined. SBC will satisfy itself that organisations comply with DPA 2018/ GDPR - due diligence		
4	**Non compliance with principles of GDPR -**			**Completion of IAR will assist**	
5	Lawfulness	SBC risks fines, compensation and reputational damage.	Determine lawful basis - may need to determine lawful basis for Special Category data.		Legal obligation Public task Contract Consent Legitimate Interest Vital interests
6	Fairness and transparency.	An individual's privacy is compromised if they are not fully informed.	PNs, consideration of fairness. Consideration to be given to sharing with other organisations.	Write PN to cover	
7	Purpose limitation.	An individual's privacy is compromised if data is shared beyond than just for the stated purpose.	Identify any required further sharing over and above for stated purpose - eg Will share some limited informaton with all partners for the purposes of monitoring outcomes/ value for money / programme evaluation. Safeguarding.		
8	Data minimisation.	An individual's privacy is compromised if more data is collected beyond than required for the stated purpose	Only collect required personal data. May need to ensure that other organisations only collect required data.		
9	Data is inaccurate at the point of collection/data entry or subsequently becomes inaccurate by being out of date	An individual's privacy is potentially compromised if information being sent to the wrong address or it could leave the individual vulnerable if their details are not up to date.	Determine how often the data needs to be refreshed. If relying on accuracy from third parties - need to ensure they take accurate info. Staff will query any data that appears inaccurate.		
10	Storage limitation.	If a retention period is not established/ complied with then information might be used for longer than necessary.	Review of retention period and compliance with retention period. Can the systems comply? - manual or technological?	Retention periods to be set. Preferable to comply via digital means rather than manual means.	
11	Integrity and confidentiality (security)	An individual's privacy is compromised if systems and processes are not adequately protected.	Configuration of SBC's systems to promote and support data integrity. If data is needed on the move then need to consider how to protect that data.		
12	Accountability	SBC risks fines, compensation and reputational damage if SBC does not ensure accountability from staff and third parties.	Contracts/MoUs/SLAs,DSAs to be completed and signed off by legal.		
13	Purpose limitation	Function creep over how personal data is processed is caused by not defining what purpose you will use your AI system. As a consequence, individuals lose control over how their data is being used.	Document each purpose for using personal data at each stage of the AI lifecycle, assess whether they are compatible with the originally defined purpose, and schedule reviews to reassess your purposes and whether they remain compatible.	Provide clear transparency information to inform individuals about your purposes from the outset. For example, in a privacy notice.	
14	Security	The unauthorised or unlawful processing, accidental loss, destruction, or damage of personal data is caused by insecure AI systems. As a consequence, individuals can suffer from financial loss, identity fraud and a loss of trust.	Document and assess the security risks, and the appropriate technical and organisational measures you will use to mitigate or manage those risks.	You must consider the security risks associated with integrating an AI system with existing systems, and document what controls will be put in place as part of the design and build phase. The level of risk will likely vary depending on the context your AI system will be used in.	
15	Meaningful human review	Tokenistic human review of outputs by AI systems may inadvertently cause solely automated decision-making with legal or similarly significant effects. As a consequence, individuals suffer from prohibited processing taking place and inaccurate and/or unfair decisions being made about them, which have legal or similarly significant effects.	Document and assess when you will incorporate meaningful human review in the decision pipeline, who will conduct the review, and what additional information they will take into consideration when making the final decision.	AI should not be used to make automated decisions. All outputs of GenAI should undergo human review and any content generated should be amended or changed where appropriate.	