CAMBRIDGESHIRE
& PETERBOROUGH
COMBINED AUTHORITY

Appendix 5

DATA PROTECTION IMPACT ASSESSMENT

Key Information

Project Name:	
Project Manager:	
Responsible officer:	
This DPIA has been completed by:	

Project Information

This should include what the objectives are, the benefits and risks to the authority plus explain why a DPIA has been completed.

Parties involved	
Please provide a list of all internal parties involved and consulted (include teams such as Finance, IT, Legal, Audit, Information Governance)	
Please provide a list of all external parties involved and consulted	
Is there or will there be a contract or similar between the authority and external parties which covers this work? *This is important to show that we have properly formed relationships which have robust agreements in place to protect the authority and our data.*	
Have you established if there are any sub-contractors involved and that suitable agreements exist *We need to be sure that we know who is processing our personal information and that we know about any subcontracting.*	

Data Flow

This is important because we need to show that we understand what is being collected or shared, who by and why, and how we make sure that this is all securely done.

What information is being collected? *It will help to provide a list and identify what special category data is collected*	
How will that information be collected and who will collect it? *Is the information being collected by email, application form, from another party etc*	
How will that information be used? *You should be clear on how it is going to be used. Will there be any profiling or automated decision making?*	
Who will information be received from? (internal and external) *This may be many sources but we need to understand the information flow between parties*	
Who will the information be shared with? (internal and external) *This may be many sources but we need to understand the information flow between parties*	
If information is being shared, how will it be shared securely? *You should identify how the information will be shared e.g direct access into a system, secure email, SFTP,*	
Who will have access to the information? *Access should be limited to only those required to have access*	

Where will the information be stored? *This should include the name of the systems for all partners, whether it is cloud or server based and if it is hosted by someone else*	
What security measures are in place? *Individual user accounts, passwords, two factor authentication, firewalls, restricted access, audit functions of the system or partner, locked cabinets*	
Do any of the parties have security or IG certification such as Cyber Essentials, Cyber Essentials Plus, ISO270001?	
How long will the information be kept for? *You should have a retention period specified by all partners.*	
How will it be destroyed? *You should have a process for how unneeded information will be disposed of, both for electronic and paper records.*	

People

This section is about the people whose data it is and how we will meet their rights under legislation

How many people will this affect? *This can be an estimate*	
What categories of people are they? *Children, adults, employees for example*	

How will people be informed about how their data is being used? *Will you be using a privacy notice, explaining to people when they sign up to a service or attend a meeting?*	
What plans are there to ensure that people's rights are met? *These are the rights of access, erasure, restriction, rectification, objection, automated decision making, data portability*	
• Can you delete data if required to?	
• Can you produce all information about a person if required to? And in what format?	
• Can you amend a record if required to?	
• Can you restrict any action being taken on a records?	
• Can you audit to see who has accessed records?	
• If the system has automated decisions, can you override these if you need a human to make the decision?	
• Can you stop processing if needed?	
Will there be any consultation of affected individuals and if so how will you conduct this consultation? *Will you be contacting and discussing with people before implementation?*	

Lawful Basis

To process any information about a person then we need to have a lawful basis or reason for doing so. We have to state this clearly in privacy notices for customers. This can be the most technical part of the DPIA so if you are not sure which is lawful basis it is then speak to the DPO and we will work with you. We need to identify the right one and we will help with that.

What is the purpose of collecting the information? *This is key because to process any personal information then we need a legal basis i.e. what allows us to do something so knowing the purpose is really key.*		
What is legal basis for processing the personal information? *It is most likely that you will be obtaining consent, having a contract with say an employee or a statutory duty. If it is a statutory duty then state what law or code of conduct makes it statutory.*	We will obtain or have obtained recorded consent	
	We have a contract with individuals to deliver this service	
	We have a legal obligation to process the information	
	We have a statutory duty to deliver the service This statutory duty is named….	
	It relates the protecting someone in a life or death situation	
	We have a legitimate interest in processing this information and have completed a legitimate interest impact assessment.	
What is the legal basis for processing special category information? *You also need to specify a basis when we are using the special category data like health, ethnicity, sexuality or religion.*	We will obtain or have obtained explicit consent in writing	
	It relates to employment or social security. This includes health and safety, maternity/paternity and sickness	
	It relates the protecting someone in a life or death situation	
	It relates to the work of a not-for-profit body like a charity, political party or charity	
	The information has already been made public by the person	
	It is required for us to make or defend legal claims	
	We have a statutory duty to deliver this service This statutory duty is named….	
	It is to deliver social care or health including occupational health	
	It is for public health reasons including monitoring and statistics or vaccination programmes	
	It is for archiving or research purposes	

Risks

Provide a list of risks and how you will manage, solve and mitigate these. To help you think about these, then we have broken down types of risks you may think of which include how they link to the principles of Data Protection.

Lawful and fair use of data **Is the legal basis correct?** **Are you using an opt out model?** **Is it clear to people what you are doing with their data?**	**Purpose** **Have you explained what the purpose is to customers?** **How will you ensure that data is not used for different purposes that a person may not expect?**	**Data minimisation** **Is there any risk that data is being collected which is not required?** **Is there any risk that more data could be shared with partners or the authority than is needed?**	**Accuracy** **Are there any risks around receiving or sharing inaccurate or old data?** **What could happen if data is not updated or is collected incorrectly?**
Retention **Is there a risk that information could be kept too long? Or too short?** **Could partners keep information without us knowing?**	**Security** **Is there a risk of people accessing information that they should not?** **Is there a risk that information will not be stored or shared securely?** **Is there a risk that information could be misused?**	**Accountability** **Is there any risk about how service users understanding how their data is being used?** **Is there a risk that privacy notices are not clear or people cannot exercise their rights?**	**Risks to the authority** **There may be risks associated with what we are doing which could impact on the authority's reputation or systems.**

Issue/Risk (indicate whether a risk to the individual or the authority)	Solution/Mitigation	Expected Outcome	How will this be monitored/evaluated

INFORMATION GOVERNANCE USE ONLY

	Sections	Comments
1	**Project Information** Are the aims and outcomes clear? Have benefits been identified?	
2	**Parties Involved–** Have all relevant teams have been identified and informed? Have all external parties been identified? Are contracts or ISAs in place?	
3	**Data Flow** Has all information to be processed been identified? Have all sources and means of processing been identified? Has appropriate security been identified? Has records management been considered?	
4	**People** Do we know who this will affect and how will they be told? Can their rights be met?	
5	**Lawful Basis** Has the lawful basis for processing been stated?	
6	**Risks and Benefits** Have all risks been identified? are risks sufficiently mitigated? What controls need to be introduced? Has a balance between the two been found? Is there a plan for monitoring?	

IG	**Overall assessment** What needs to change? if anything	

SIGN OFF			
Sign off	Title	Signature	Date
	Lead Officer		
	Director/Senior Responsible Officer		
	Data Protection Officer		
	SIRO		