Privacy Impact Assessment

<Provision of Intensive Home Visiting Service>

APPENDIX A

Privacy Impact Assessment – Screening Questions

Question	Y/N	Additional Comments (please give reasons for either a 'yes' or' no 'answer here
Is there a requirement under GDPR to carry out a PIA? NB if there is a legal requirement to carry out a PIA there is no requirement to complete the remaining questions.	Y	The provider will be responsible for the creation of new child health records along with new client records of individuals referred into the service
Will the project involve the collection of new information about individuals?	Y	The project is being re-procured and a PIA is being carried out to ensure data processing complies with GDPR. The provider will be required to collect new information and create records for clients referred in to the service.
Will the project compel individuals to provide information about themselves?	Y	Clients are required to give personal and sensitive data in order to receive the service
Will information about individuals be disclosed to third party organisations or people?	Y	Information about individuals will be disclosed to third party organisations in instances when individuals are referred onto other services to address particular health needs. However, this will only be done with the individuals consent
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	N	

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Y	The provider may discharge the individual before the completion of the service The provider may have to make onward referrals in the best interest of the individuals involved e.g safeguarding
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, health or information concerning an individual's sex life or sexual orientation or other information that people would consider to be private.	Y	The provider will be required to collect personal and sensitive information within the health records they keep on the individual and child
Will the project require you to contact individuals in ways that they may find intrusive?	N	
Will the data be held in relation to children or vulnerable adults?	Y	Health records for the children will be kept by the provider

APPENDIX B

Privacy Impact Assessment

Step 1 – Requirement for PIA – issues to be addressed

To Include:
- Project Aim and Objectives
- Benefits to the organisation, to individuals and to other parties of personal data
- Links to any relevant project documentation
- Summary of Identified Need for PIA (can draw on answers to the screening questions).

Background
Public Health in DCC will be re-procuring an Intensive Home Visiting service, which will work with some of the most vulnerable young mums to offer a more intensive health visiting support service to address their and their child's health needs.

Project aims and objectives:
The overarching aim of the Intensive home visiting service is to:
- protect and promote the health and wellbeing of children in the early years
- Reduce health inequalities

Key objectives of the service is to**:**
- Improve the outcomes in pregnancy by helping women improve their ante-natal health and the health of their unborn baby
- Improve children's subsequent health and development by helping parents to provide consistent, competent care for their children
- Support parents to access education, employment and training opportunities
- Support the mother and child to promote strong attachment, bonding and emotional and mental health of both
- Work with fathers/partners as far as possible, supporting them to be effective co-parents
- Engage with the local community to develop services where needs have been identified
- Be able to demonstrate cost effectiveness and value for money

Benefits to the organisation, to individuals and to other parties of personal data

While most mothers are able to have their needs met using mainstream health visiting services, some mothers (particularly those with certain vulnerabilities) require a more intensive service to help meet their complex needs and address the service aims and objectives outlined above. Those in need of more intensive support to meet their needs may include:

- Young mums under the age of 20
- Those with a history of substance misuse
- Those with identified learning disabilities
- Those with previous or current history of mental health problems / personality disorder
- Those with previous safeguarding involvement
- Those who have previously been or are a victim of domestic abuse
- Ex-offenders
- People who are homeless
- Parent/infants where there are complex health needs

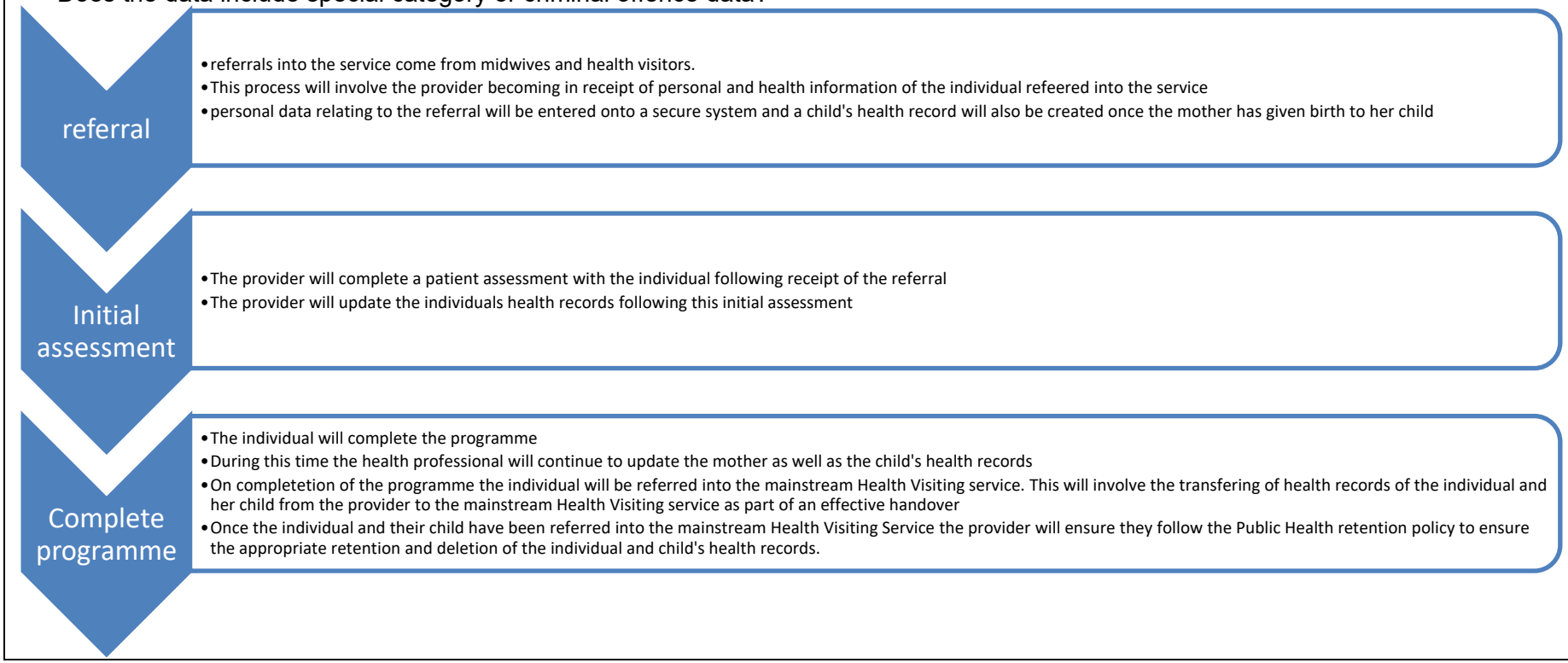
Summary of need for PIA

Personal and sensitive data will be collected and health records will be kept by the provider in order for individuals to be referred and to access the Intensive Home Visiting Service. The Council is performing a PIA to ensure the re-procurement of the Intensive Home Visiting Service is compliant with GDPR requirements and to ensure privacy risks are minimised.

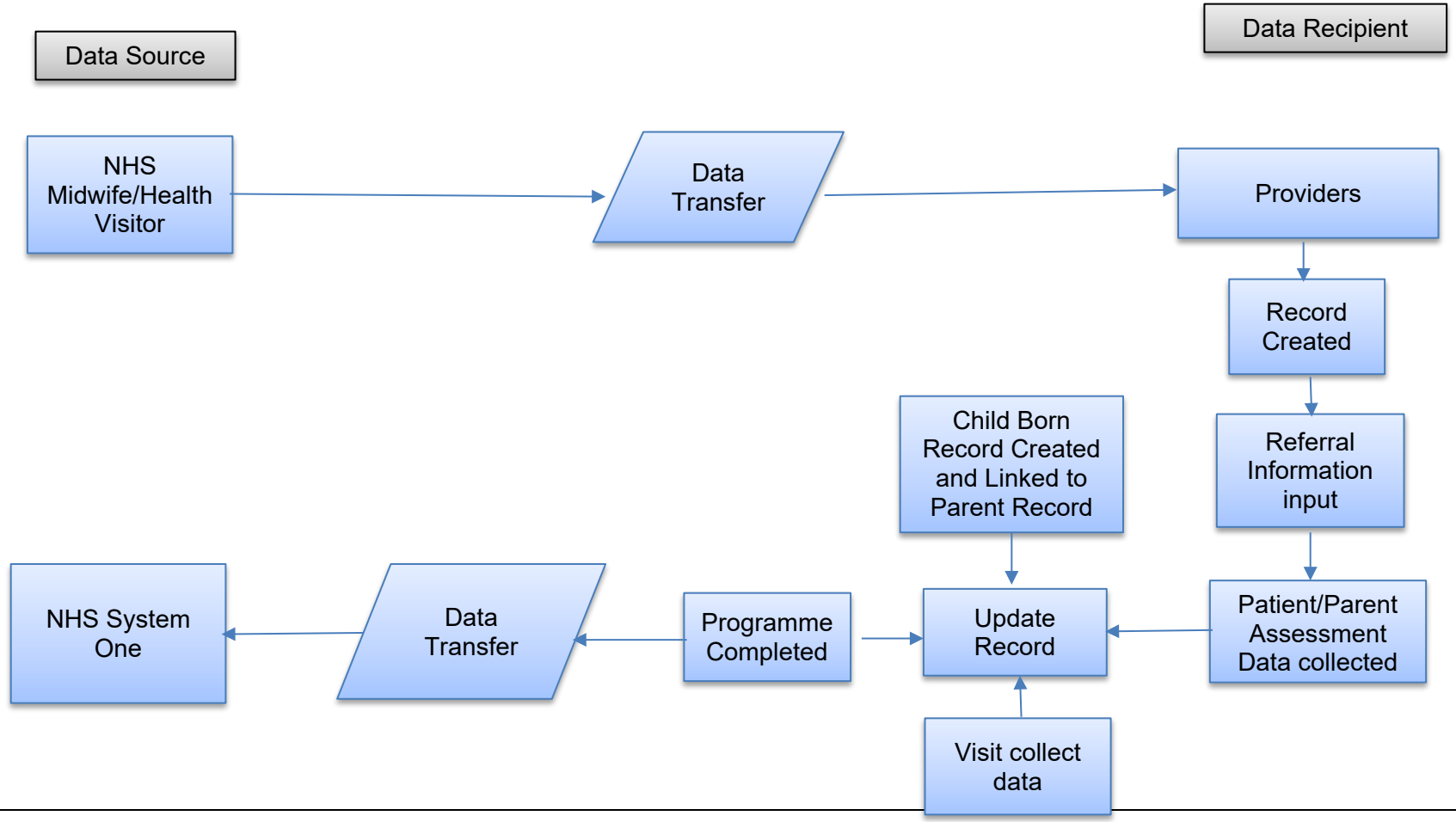
Step 2 – Information Flows/Nature of processing

To Include:

- Description of collection, use, retention and deletion of personal data- is any sharing of data involved?
- Explanation of data flows – diagram or description detailing: controllers and processors, storage location and storage method, personal data fields collected, individual/team/organisational access to personal data(audit trail), security measures for storage and transfer of data
- Number of individuals likely to be affected by the project-do they include children or other vulnerable groups?
- A flow diagram is likely to be helpful here.
- Does the data include special category or criminal offence data?



Information flow require mapping out are the referrals transferred electronically from one secure system to another?



Reason for Processing - To put in place a service that provides vulnerable young mothers and their children with additional intensive health visiting support. Processing of personal and special category data is necessary to ensure that they receive the most appropriate and the most effective support and that care is continuous during transition between services.

Data Processor: The provider of the Intensive Home Visiting service

Data Controller: Joint between Derbyshire County Council and the provider

Data Security – Providers will have to ensure that appropriate security measures are in place to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Access to personal data will be limited to employees whose role requires access for service and treatment purposes. Data security requirements are covered in the contractual arrangements and compliance with Audits requirements with regards to information security.

International Transfers – Personal data will not be transferred or stored outside of the UK.

Patient Discharge – On discharge from the service the provider will refer the individual and child to the mainstream Health Visiting Service using a secure method of onward referral in order to protect the data of both the individual and their child.

Data Retention - Providers will only retain personal data for as long as necessary to fulfil the purposes it is collected for, including the purposes of satisfying any legal, accounting or reporting requirements. Throughout the programme the provider will adhere to Derbyshire County Councils (Data controllers) Public Health retention policy to ensure the safe and appropriate retention and deletion of personal data of the individuals engaged within the service.

Current National companies data retention periods.

Data relating to Health – Period of 8 years from end date of treatment.

Data relating to Contractual Data – Period of 6 years from the end date.

NHS bodies will retain record in line with NHS data retention regulations – see attached.

Step 2 – Consultation Requirements

Identify whether internal and/or external consultation is required to address privacy risks

- Stakeholders to be consulted
- Method of consultation

Procurement - Providers will be required to obtain Cyber Essentials or equivalent as per the Selection Questionnaire that will be within the procurement documentation.

DCC Audit Services - will be required to undertake an Information Security Audit in order to ensure the appointed provider of the Intensive Home Visiting Service complies with all of the Information Security Management System Policies and Procedures.

Audit Services to establish the provider has the appropriate levels of security in place to manage, protect and safeguard patient information. To report on findings of potential non-conformities for the provider to consider findings and agree a timetable for correction. Prior to final report being referred to the County Councils Director of Finance and ICT for consideration.

Contract management meetings will include an operational review of any incidents relating to individuals

Consultation will be undertaken with the successful provider to assess privacy risks.

Part B Steps 3 to 4 – Identify Privacy Risks, Solutions and Approval

Privacy Risk	Risk to Individuals & organisation	Risk initial score	Action Identified	Target Score (after applying actions)	Risk Control Plan (Treat/Control/Tolerate/Accept/Terminate/Transfer)	Evaluation: is the final impact on individuals and the organisation after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Approved By
Disclosure of the personal sensitive data that is required to deliver the service.	Harm and distress if released, unauthorised access or used for different purposes Inappropriate /excessive disclosure of personal and sensitive data. Financial and reputational damage. Legal action	1x 4 =4	Compliance with Data Protection Act laws. Providers have procedures, protocols and policies in place for staff to comply with DPA including an appropriate privacy notice Information Security Audit from DCC will be required.	4	Control	Yes	

Data is accessed by unauthorised persons and used or shared inappropriately	Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information Financial and reputational damage. Legal action	1x 4 = 4	Ensure that authorised persons have been trained in Information Governance procedures and protocols and understand how to report any security breaches to the data controller If possible, ensure that system has an audit trail that enables access to records to be monitored	4	Control	Yes	
Data held for longer than lawful retention period	Data is kept longer than is necessary.	1x1 = 1	Provider ensures they comply with the relevant retention policies and have the means to adequately destroy records at the end of the period.	1	Treated/Control	Yes	

Step four: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Compliance with Data Protection Act laws; Providers have procedures, protocols and policies in place for staff to comply with DPA	Tender process	Procurement and DCC PH ensure that successful bid meets contract requirements
Information Security Audit from DCC will be required.	Following award of contract	DCC Audit Services
Ensure that authorised persons have been trained in Information Governance procedures and protocols and understand how to report any security breaches to the data controller	Point of award and throughout contract	Successful Provider
If possible, ensure that system has an audit trail that enables access to records to be monitored	Point of award	Successful Provider
Provider ensures they comply with the relevant retention policies and have the means to adequately destroy records at the end of the period.	End of contract	Successful Provider

Contact point for future privacy concerns
Date of consideration by IGG

APPENDIX C

Linking the PIA to the GDPR principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

- Have you identified the purpose of the project and which lawful basis applies? C & E
- Is the processing of the data necessary in terms of GDPR? Y
- How will you tell individuals about the use of their personal data?

Providers will obtain consent from the individual using a method of consent that they should be able to evidence (for example, completing a written consent form)

- Do you need to amend your privacy notices? N
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? – written consent should be obtained. The intensive home visiting service is an opt-in service. Therefore, if individuals refuse to consent for the provider to process personal N/A

information then there is no obligation for the individual to complete the service.

- If special categories of personal data have been identified have the requirements of GDPR been met? Y

As the Council subject to the Human Rights Act, you also will where privacy risk are especially high need to consider:

- Will your actions interfere with the right to privacy under Article 8? N
- Have you identified the social need and aims of the project? Y
- Are your actions a proportionate response to the social need? Y

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data? Y
- Have you identified potential new purposes as the scope of the project expands? N
- Does your Privacy Notice cover all potential users? Y

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the quality of the information good enough for the purposes it is used? Y
- Which personal data could you not use, without compromising the needs of the project?

Health Visitors should apply their professional principles in accessing only the personal data relevant to the current situation

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary? Not procuring software. N
- How are you ensuring that personal data obtained from individuals or other organisations is accurate? Through contractual requirements, collecting data for the sole purpose of the service and ensuring the data is maintained and accurate. Y
-

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

- What retention periods are suitable for the personal data you will be processing?

Provider Retention periods Health – Period of 8 years from end date of treatment.

- Are you procuring software that will allow you to delete information in line with your retention periods? Y

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under GDPR.

- Will the systems you are putting in place allow you to respond to subject access requests more easily? Contractual requirements will be in place to comply. Y
- Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten). Contractual requirements are in place to comply. Y
- If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose? There is no marketing involved in the contract. NA

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified? Contractual requirements will be in place to comply Y
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

The procurement is not for a new system, it is to deliver a service. The Provider will ensure appropriate training is given to staff so that data is kept safe e.g. password kept safe and not shared, locking screens and logging out of systems, only accessing records when required.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate

level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA? Ensure that supplier will not be transferring data outside of the EEA | N

- If you will be making transfers, how will you ensure that the data is adequately protected?

Not applicable