DERBYSHIRE County Council

Information Security Document

Live Life Better Derbyshire Stop Smoking Database Privacy Impact Assessment

Version 1.0

Version History			
Version	**Date**	**Detail**	**Authors**
1.0	12/12/2017	First Draft for consideration by Procurement	

CONTENTS

Contents	Page
Section 1 - PIA Screening Questions	3
Section 2 Step 1 – Outline Requirement for PIA	4
Section 2 Step 2 Data Flows	5
Section 2 Step 2 Consultation Requirements	6
Section 2 Step 3 – Identify Privacy Risks	7
Section 2 Step 4 – Identify Privacy Solutions	8
Section 2 Step 5 and 6 – Sign Off and Integrate PIA Outcomes into Project Plan	9
Section 3 - Linking the PIA to the Data Protection Principles	10

Privacy Impact Assessment – Project CTP781 THESEUS system (Stop Smoking), Public Health

Section 1 - PIA Screening Questions

Question	Y/N	Additional Comments (optional)
Will the project involve the collection of new information about individuals?	Y	Creation of client records collecting personal data at point of referral and recording of sensitive data throughout health intervention period
Will the project compel individuals to provide information about themselves?	Y	Participation in the health intervention requires provision of personal and sensitive data for managing clients and monitoring client outcomes
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y	The health intervention programme will be directly commissioned by DCC
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	This is a new data collection that is being collected solely for the intended purpose of managing clients and monitoring outcomes and will not be used for any other purposes
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?	N	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	Y	Personal and sensitive data will be collected
Will the project require you to contact individuals in ways that they may find intrusive?	N	Individual chooses how to be contacted

Section 2 Step 1 – Outline Requirement for PIA

Background: Public Health in DCC will be providing a new integrated health and wellbeing service (Live Life Better Derbyshire, LLBD) for the Derbyshire population that covers all aspects of health and wellbeing including weight management, physical activity, smoking cessation, alcohol consumption and mental wellbeing. The stop smoking service element of the service requires a client case management system and booking system to support service delivery and local & national reporting requirements.

Aim: The LLBD stop smoking service aims to support people to stop smoking and in turn improve their health and wellbeing and reduce the risk of developing a long term condition.

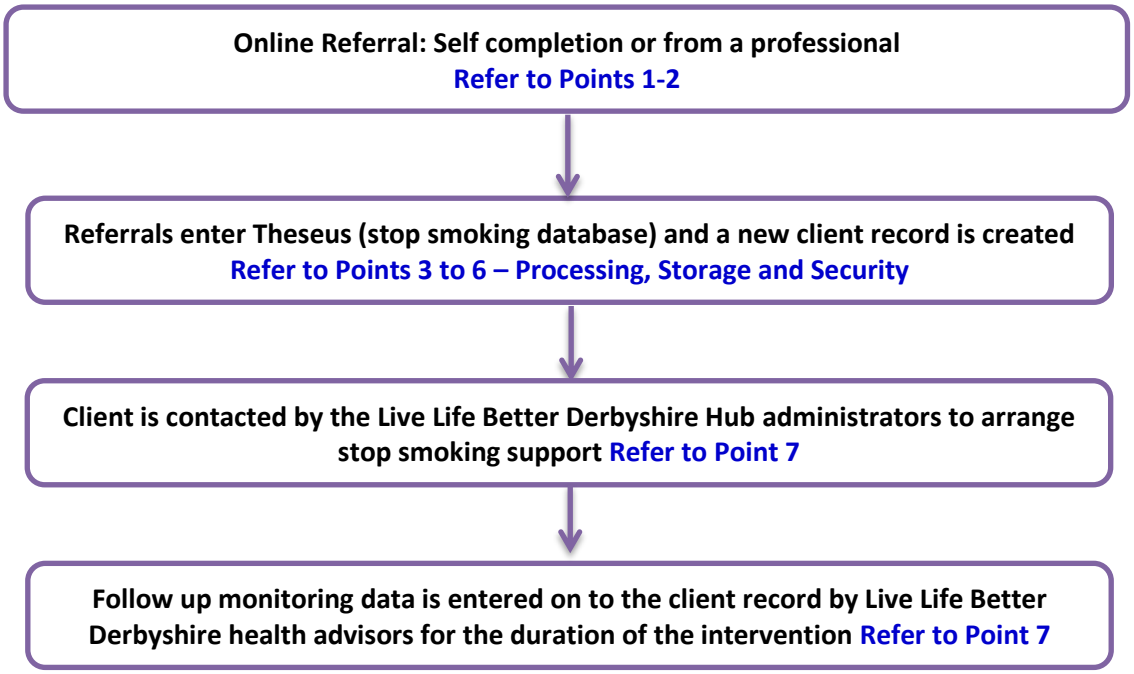
Objectives: To provide a client case management system for the LLBD health advisors, recording client details, intervention details and pharmacotherapy issued. Also to provide a booking system to allow the LLBD Hub administration staff to book clients with advisors and managers to view service capacity and book team meetings/CPD.

Benefits: Lifestyle/Health Improvement services are important in the prevention and management of many long term diseases, including cardiovascular disease, respiratory disease, diabetes and cancer. Providing cost-effective and evidence based services to secure sustained lifestyle behaviour change, among those most at risk of poor health outcomes, supports population-level health improvement and reduces inequalities, thereby reducing the longer term costs to the health and social care system.

Business Need: A client case management and booking system is critical to successful delivery of the service. LLBD health advisors require a system to record clients details, intervention details, details of pharmacotherapy provided. A booking system is also essential in ensuring the effective processing of referrals and booking clients into clinics. The booking tool will also provide information to managers of service capacity and allows team meetings and CPD to be booked into an advisors calendar.

Requirement for PIA: To achieve the above it will be necessary to collect and store data relating to individuals and their health and wellbeing, therefore it is essential to minimise any inherent privacy risks this could present and reduce the risk of harm to both individuals and organisations. The screening process identified that new information about individuals containing both personal and sensitive data will be collected at the point of referral and throughout health intervention period, that provision of this information is mandatory in order to access and benefit from the service, and that there will be new data controller and data processor organisations.

Section 2 Step 2 Data Flows – Stop Smoking Service Information Flow Diagram



1. **Personal & Sensitive Data Fields Collected**

Contact Details	Name, Address, Email, Postcode, DOB, Phone, Preferred Contact Method, GP Practice
Monitoring Details	Gender (if Female, Indicate if Pregnant/Breastfeeding for specialist support), Ethnicity, Prescription eligibility
Employment Details	-Employment Status and Occupation Code (for identifying R&M)
Intervention Details	CO readings, Pharmacotherapy, Completion status, Client satisfaction
Mental Health	In receipt of secondary MH services (Y/N) Self-rated MH problem/illness (Y/N)

2. **Positive Opt in:** Clients are provided with a privacy notice at the end of the online referral process. When contacted by Live Life Better Derbyshire Hub administrators clients are directly asked to confirm their consent using a standardised client statement and this is recorded in the client record on the Theseus database.
3. **Data Processor**: Cyber Media Solutions Ltd, Opus House, Priestly Court, Staffordshire Technology Park, Stafford ST18 0LQ
4. **Data Controller**: Derbyshire County Council
5. **Storage Method**: Data at Rest is stored on Clustered Shared Volumes and encrypted by Microsoft BitLocker using the Advanced Encryption Standard (AES) 256-bit algorithm. Data in Transit is transmitted using an encrypted channel via the use of SSL (TLS) certificates using cryptographically strong protocols and ciphers.
6. **Storage Location:** Data will be held in an ISO27001:2013 certified UK data centre (located in a former Bank of England bullion vault: ServerBank Data Centre, Bank Chambers, Faulkner Street, Manchester M1 4EH).

7. **Access to Referral Records:**

a. **Client Booking Contact Details:** LLBD Hub administrators will be able to access client contact details in order to book clients onto stop smoking support clinics with an LLBD health advisor. Managers will be able to view clinic capacity and arrange staff meetings.

b. **Client Intervention Records:** Only LLBD health advisors will be able to access the client stop smoking intervention record. Advisors will have individual logins and passwords which will create an audit trail. All advisors will be DCC employed.

c. **Monitoring data:** performance data will be fully anonymised and accessible to Public Health Managers in the LLBD team

8. Number of individuals likely to be affected by the project is 2000+ per year.

Section 2 – Consultation Requirements
DCC Audit Services have undertaken a full Data Protection and ISO27001:2013 audit of the 3rd party supplier which has been signed off as complete therefore the 3rd party supplier meets required security standards

Section 2 Step 3 – Identify Privacy Risks

Privacy Issue	Risk to Individuals	Compliance Risk	Organisation Risk
Disclosure of the personal and sensitive data that is required for delivery of the service	Harm and distress if released, unauthorised access, or used for different purposes Inappropriate/excessive disclosure of personal and sensitive data	DPA 1 – Fair & lawful processing DPA 2 – Specified lawful purpose DPA 3 – Adequate, relevant and not excessive DPA 7 – Appropriate measures against unauthorised/unlawful processing	Breach of DPA Financial penalties. Reputational damage and loss of public trust
Storage and processing of personal/sensitive data	Concern to over how/where personal data are stored and processed	DPA 7 – Appropriate measures against unauthorised/unlawful processing DPA 4 – Accurate, up to date	Breach of DPA Loss of data Unauthorised/unlawful use Inaccurate data
Subject Access Requests	Unable to access the data on their client record	DPA 6 – system allows for right to access personal data	Breach of DPA Failure to respond to requests
Retention and Deletion of data	Concern to individual over retention of data following exit from the service	DPA 4 – Accurate, up to date DPA 5 – Data shall not be kept for longer than necessary	Breach of DPA Breach of retention schedule Old and inaccurate data

Section 2 Step 4 – Identify Privacy Solutions

Privacy Issue	Solution(s)	Risk Eliminated/ Reduced/Accepted	Evaluation
Disclosure of the personal and sensitive data that is required for delivery of the service	-Clear and Accessible Privacy Notice -Positive opt in to the service -Role based access to restrict certain modules to LLBD advisors only -Staff trained in the new system and clear on usage and data flows -Staff undertake training in Information Governance -Data used for monitoring purposes will only be accessible at a fully anonymised level	Reduced Reduced Reduced Reduced Reduced Eliminated	Measures are justified and proportionate to risk
Storage and processing of personal/sensitive data	-Data fully encrypted in transit and at rest -Data stored in ISO certified services on dedicated server -Adherence to Incident Management policy and defined procedures for recording and monitoring security incidents -Individual logins and adhere to DCC password protocols	Eliminated Eliminated Reduced Reduced	Measures are justified and proportionate to risk
Subject Access Requests	-Ensure the system allows for response within 40 days -Staff will receive training on appropriate note taking techniques	Eliminated Reduced	Measures are justified and proportionate to risk
Retention and Deletion of data	-System allows for records to be amended/updated -Documented Disaster Recovery plan and Certificate of Destruction for hard drives and manual records, and return or delete clause included in contract -Data retained according to the Public Health Retention Schedules -Right to deletion included in the privacy notice	Eliminated Eliminated Eliminated Eliminated	Measures are justified and proportionate to risk

Section 2 Steps 5 and 6 – Sign Off and Integrate PIA Outcomes into Project Plan

Risk	Solutions Approved?	Approved By	Actions to be taken	Date for completion	Responsibility
Disclosure of the personal and sensitive data that is required for delivery of the service	Yes	Anne Hayes	-Write a clear privacy notice -Agree with supplier how this will be accessible to clients -Staff training on Theseus system -Staff training on IG	1st Dec 1st Dec 1st Dec Part of induction	 LLBD Team LLBD Team
Storage and processing of personal/sensitive data	Yes	Anne Hayes	-Conduct 3rd party supplier audit -Identify supplier has a documented Incident Management policy and recording system -Ensure individual login with password	Complete Complete 4th Dec	Audit Audit
Subject Access Requests	Yes	Anne Hayes	-Ensure system is compliant with subject access requests and existing DCC policy and procedures -Staff training on note taking	1st Dec March 2018	
Retention and Deletion of data	Yes	Anne Hayes	-Identify Disaster Recovery plan and Certificate of Destruction -Specify data deletion or return -Include in PH retention schedules -Include right to deletion in privacy notice	Complete 21st Dec 1st Dec 1st Dec	

Contact for future privacy concerns

Section 3 - Linking the PIA to the Data Protection Principles

Principle 1 - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: **a) at least one of the conditions in Schedule 2 is met, and** **b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**	
Have you identified the purpose of the project?	Yes
How will you tell individuals about the use of their personal data?	Privacy Notice
Do you need to amend your privacy notices?	Yes
Have you established which conditions for processing apply?	Yes
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?	Consent is being electronically recorded at point of referral but is not a condition of access, as the lawful basis for processing is Schedule 2 (2) and Schedule 3 (4) and Article 6 (1) and 9(2) of GDPR
If your organisation is subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	No
Have you identified the social need and aims of the project?	Yes
Are your actions a proportionate response to the social need?	Yes

Principle 2 - Personal data shall be obtained only for one or more specified 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?	Yes
Have you identified potential new purposes as the scope of the project expands?	n/a

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?	Yes
Which personal data could you not use, without compromising the needs of the project?	Minimum data collected

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?	Yes
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Staff are required to check personal details at point of referral, booking and at point of intervention

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	
What retention periods are suitable for the personal data you will be processing?	6 years
Are you procuring software that will allow you to delete information in line with your retention periods?	Yes

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	n/a
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	n/a

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?	Yes
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	Internal training for LLBD staff

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?	No
If you will be making transfers, how will you ensure that the data is adequately protected?	n/a