Privacy Impact Assessment – Project CTP782 OCTIGO system (First for Wellbeing), Public Health

Part A - 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 and analysed
Will the project require you to contact individuals in ways that they may find intrusive?	N	The client Individual chooses how to be contacted

Part B 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. New clients will access the service through a single point of referral (via website or Freephone) to receive advice/information, signposting to external services and access to interventions delivered in-house.

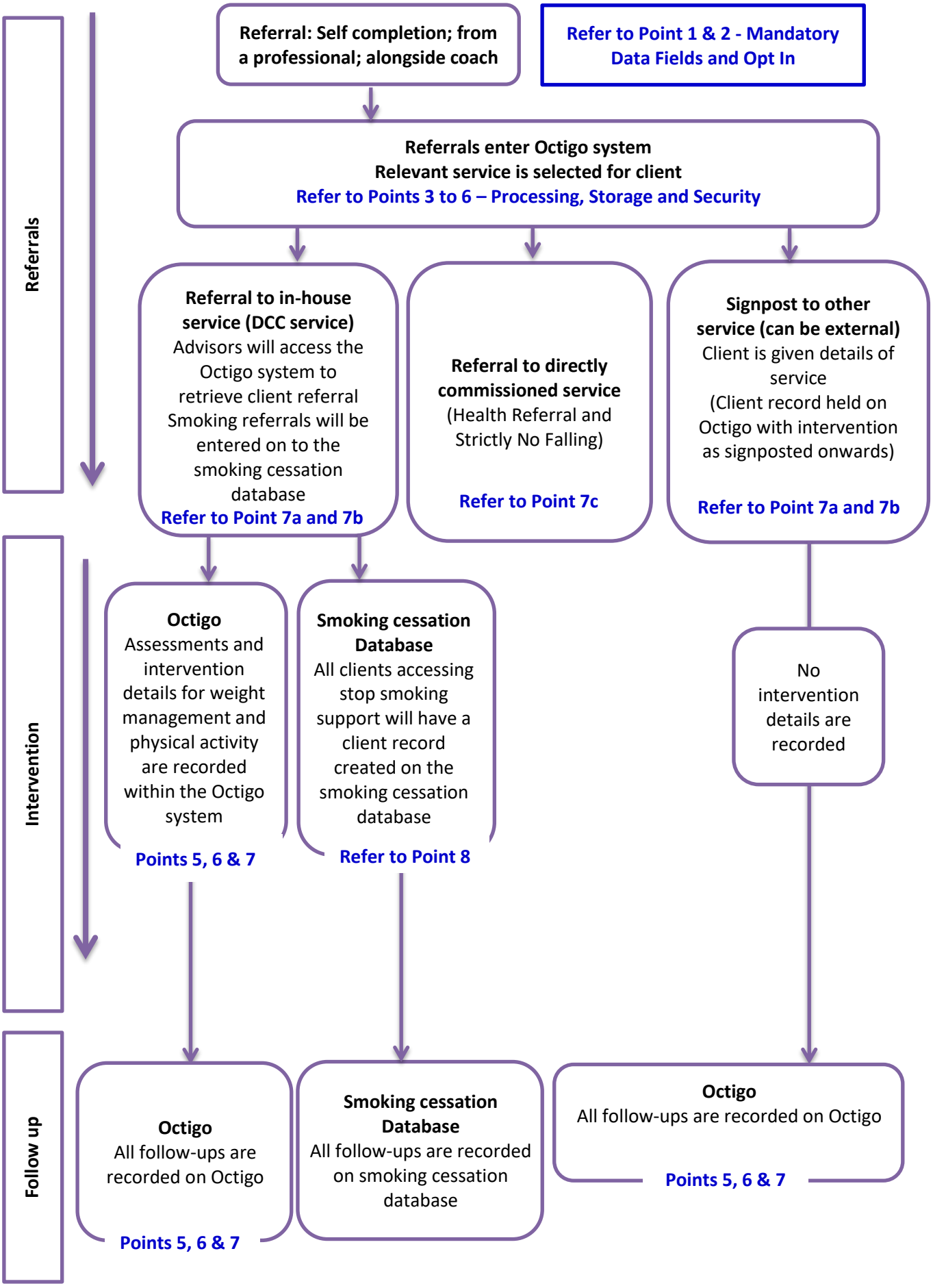
Aim: The LLBD service aims to effect a dramatic improvement in the physical, emotional and social health and wellbeing of the people of Derbyshire through sustained lifestyle behaviour change

Objectives: To accurately identify and prioritise client health and wellbeing needs, to deliver an effective service, to deliver value for money
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 fit for purpose IT solution is critical to successful delivery of the service. To accurately identify and prioritise client health and wellbeing needs requires an established, evidence based self-assessment tool that can be used independently or with a wellbeing coach for those who need additional support. The assessment tool is a key element of the new service that needs to reliably assess an individual's needs and motivations based upon responses to a range of questions, ensuring the right services are provided and prioritised in a personal plan.

Octigo health and wellbeing assessment tool: Following a comprehensive evidence search and consultation with public health networks, an established system solution was identified that met the above requirements. The 'Octigo' tool supports the 'First for Wellbeing' programme in Northamptonshire. Based upon the clients responses to a range of health and wellbeing questions, the tool produces a 'priority needs map' showing individual needs in sequence or priority order increasing the effectiveness of the wellbeing coaches' role as an automatic algorithm approach. The customer relationship management (CRM) function engages with the individual to deliver motivational messaging to support behaviour change. The case management system hosts a booking system for advisors to manage their daily schedules and receive alerts, reducing administration time and maximising the time given to providing frontline support. The integrated reporting functionality of the tool enables programme evaluation to demonstrate the effectiveness of the intervention.

Requirement for PIA: To achieve the above it will be necessary to collect and store a wide variety of 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.

Part B Data Flows – Live Life Better Derbyshire (LLBD) Information Flow Diagram



The LLBD Information Flow Diagram summarises the service structure and identifies the points at which data will be collected and held. Further details on storage location, method and transfer, personal data fields collected, individual/team/organisational access to personal data, security measures and controllers and processors are given below.

1. **Mandatory Data Fields Collected at Point of Referral**

Contact Details	Name, Address, Email, Postcode, DOB, Phone, Preferred Contact Method
Monitoring Details	Gender (if Female, Indicate Pregnant/Not pregnant for accessing Stop Smoking specialist) Ethnicity, Parent or Carer, Sexuality
Employment Details	-Employment Status -In receipt of benefits (in case eligible for assistance)
Health & Lifestyle	-Do you smoke? If Yes Indicate: I want to quit/I would benefit from advice -Do you drink alcohol? If Yes Indicate: How often/Units per day -Do you have concerns about your weight? -Are you receiving mental health services? -Do you have a long term health condition?
Social Capital	(Agree/Disagree): -I often feel lonely -I have few chances to socialise with people -I do not feel close to people in my area -I struggle to mix with people
Emotional	(Agree/Disagree): -I feel optimistic about the future -I feel useful -I feel relaxed -I deal with problems well -I think clearly
Financial	Are you worried about money? If Yes, Indicate Debts/Losing Home/Paying Bills/Rarely money to do things I enjoy
Housing	At Risk/Homeless/Require support/No Support

2. **Opt in:** Clients will be required to agree to the LLBD Fair Processing and Privacy Notice explaining why and how data are used, how data are secured and shared, and individual privacy rights. Data are only shared for referral to services provided by external partners.
3. **Data Processor**: LGSS Shared Services, 4 Angel Street, Northampton, NN1 1ED
4. **Data Controller**: Derbyshire County Council
5. **Storage Method**: Data is stored using encryption both in transit (using AES 256 SSL generated from 4096bit encrypted key using TLS v1.2) and at rest (AES 256 using set of 4096bit encryption keys).
6. **Storage Location:** Data will be held in an ISO27001:2013 certified Amazon Web services within a UK data centre. Data will be stored in a logically isolated network dedicated solely to DCC services, servers and data and will be managed remotely.
7. **Access to Referral Records:**
    a. **Client Referral Data:** Only LLBD advisors will be able to access the client referral record. Advisors will have individual logins and passwords which will create an audit trail. All advisors will be DCC employed.
    b. **Monitoring data:** performance data generated by Octigo will be fully anonymised and accessible to Public Health Managers in the LLBD team

c. **Health Referral and Strictly No Falling:** Referral forms containing minimum data required for contact will be sent from the LLBD advisors via encrypted email to commissioned providers. The original client referral record will remain within the Octigo system. A DSA will be in place.

8. **Stop Smoking (SS) Database:** Only data relevant to the SS service is transferred to the client record (referral data). This is inputted manually into the smoking database by DCC staff. Client records are held on the smoking database. This system has already been procured and undergone internal audit.

9. Number of individuals likely to be affected by the project

Part B – Consultation Requirements
Internal consultation to be carried out with DDC Audit Services to include a full Data Protection and ISO27001:2013 audit of the 3rd party supplier. Audit Services seek assurance that applications which process/ hold or transmit financial transactions or personal information have an appropriate level of information security in place. The following elements will be included in the audit of the First for Wellbeing programme:- Head office due diligence visit:- ensure the supplier has appropriate technical and security measures in place to ensure a level of security appropriate to the risk including: • Evidence of Information Security policies and procedures and their means of implementation e.g. recruitment procedures, physical access controls, acceptable use policies, use of encryption, incident reporting and management etc. • Review of the application, where Access to a 'test' system will be required which is based on the current 'live' version including full functionality so that Audit can run a series of test scripts through the application to evidence certain aspects such as, but not limited to:- • transactions/ data are correctly recorded; • an effective Audit Trail is maintained; • data validation is operational on key fields; • basic security procedures are operational including password protocol and privilege management etc A summary of potential non-conformities should be issued to First for Wellbeing for comment including assessment of the perceived risk level. The supplier can then consider the findings and incorporate a timetable for correction of the matters raised before being referred to the County Council's Director of Finance & ICT for consideration.

Part B Step 3 – **Privacy Risks**

Privacy Issue	Risk to Individuals	Compliance Risk	Organisation Risk
1) Breadth of sensitive data items required to be collected due to service nature	• Concern to individual over amount of data being collected, stored and accessed • Harm and distress if released, unauthorised access, or used for different purposes	• DPA 1 – Fair & lawful processing • DPA 2 – Specified lawful purpose - clear statement of proposed uses • DPA 3 – Adequate, relevant and not excessive	• Breach of DPA • Loss of reputation and service confidence due to client concerns on amount of data being collected, stored and accessed
2) Disclosure of personal and sensitive data due to service nature and data required	• Inappropriate/excessive disclosure of personal and sensitive data	• DPA 7 – Appropriate measures against unauthorised/unlawful processing • DPA 3 – Adequate, relevant and not excessive	• Breach of DPA • Unauthorised/excessive use • Loss of reputation due to disclosure
3) Storage and processing of personal/sensitive data	• Concern to individual over how/where their details 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
4) Transfer of data to the Stop Smoking database	• Harm and distress if released, unauthorised access, or used for different purposes • Concern over additional records created on a separate system	• DPA 7 – Appropriate measures against unauthorised/unlawful processing • DPA 3 – Adequate, relevant and not excessive • DPA 4 – Accurate, up to date	• Breach of DPA • Loss of data • Unauthorised/unlawful use • Inaccurate data
5) Referral to Health Referral Scheme/Strictly No Falling	• Concern over sharing data with external organisation	• DPA 7 – Appropriate measures against unauthorised/unlawful processing • DPA 3 – Adequate, relevant and not excessive • DPA 4 – Accurate, up to date	• Breach of DPA • Loss of data • Unauthorised/unlawful use • Inaccurate data
6) Subject Access Requests	• Unable to access the data being held on record	• DPA 6 – system allows for right to access personal data	• Breach of DPA • Failure to respond to requests

7) Retention and Deletion of data	• Concern to individual over retention of data following exit from the service	• DPA 5 – Data shall not be kept for longer than necessary	• Breach of DPA • Breach of retention schedule

Part B Step 3 –**Privacy Solutions**

Privacy Issue	Solution	Risk Eliminated/ Reduced/Accepted	Evaluation
1)	**DPA 1 and 2** - Explicit consent should not be 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. Clients should not be given a false sense of control when data is a pre-requisite for accessing the service. However, there is a clear need to inform and assure clients their data will be looked after: **1)** A Clear and Accessible Privacy Notice to which clients must positively agree (opt in): -a specific statement, ideally should open as a dialogue box with the acceptance incorporated, name organisation and any 3rd parties -including: Why this data is being collected, The purposes for which it will be used, What will and will not be shared, Who has access to personal level data, How to withdraw **DPA 3 -** 2) Review each data field, log the justified purpose and check it meets privacy notice Option for client non-response to questions where not required for receipt of service/entry into 'client contract'	Reduced Eliminated	Measures are justified and proportionate to risk
2)	**DPA 7 -** 1) Role based access to restrict certain modules to LLBD advisors only 2) Staff will be fully trained in the new system and clear on usage and data flows 3) Staff will undertake training in Information Governance including telephone procedures **DPA 3 -** Data used for monitoring purposes will only be accessible at a fully anonymised level	Reduced Reduced Reduced Eliminated	Measures are justified and proportionate to risk
3)	**DPA 7 -** 1) Data will be fully encrypted in transit and at rest 2) Data will be stored in ISO certified services and stored in dedicated server 3) There will be an Incident Management policy and defined procedures for recording and monitoring any security incidents 4) Staff will have individual logins and adhere to DCC password protocols	Eliminated Eliminated Reduced Eliminated	Measures are justified and proportionate to risk

	DPA 4 – 5) The system will enable staff to amend data where necessary 6) Where possible fields will have set validation e.g. DD/MM/YYYY, weight/height	Eliminated Reduced	
4)	**DPA 7 –** 1) The Stop Smoking database is stored XXX and encrypted 2) Access to personal data is restricted to health advisors with individual logins **DPA 3 -** Only the minimum data required for the service will be transferred by LLBD advisors **DPA 4 –** Clients will be asked to confirm any details when accessing the stop smoking service to ensure accuracy of data	Eliminated Reduced Reduced Reduced	Measures are justified and proportionate to risk
5)	**DPA 7 –** 1) Referrals will be transferred using the DCC encrypted email service 2) Access to personal data is restricted to the health referral/strictly no falling scheme advisors 3) A data sharing agreement will be implemented **DPA 3 -** Only the minimum data required for the service will be transferred **DPA 4 –** Clients will be asked to confirm any details when accessing the health referral service to ensure accuracy of data	Reduced Reduced Reduced Reduced Reduced	Measures are justified and proportionate to risk
6)	**DPA 6 –** 1) The existing DCC procedures for Subject access data requests should be applied to the LLBD service 2) It should be ensured the system allows for response within 40 days 3) Staff will receive training on appropriate note taking techniques	Eliminated Eliminated Reduced	Measures are justified and proportionate to risk
7)	**DPA 5 –** 1) A documented Disaster Recovery plan and Certificate of Destruction for hard drives and manual records, and return or delete clause included in contract 2) Data will be stored according to the Public Health Retention Schedules 3) The right to deletion will be included in the privacy notice	Reduced Reduced Eliminated	Measures are justified and proportionate to risk

Part B Steps 6 and 7 – Sign Off and Integrate PIA Outcomes into Project Plan

Approved Solution?	Approved By	Actions to be taken	Date for completion	Responsibility
1) Y/N		a) Write a clear privacy notice b) Agree with supplier how this will be accessible to clients c) Review and list all required data fields alongside their purpose for collection d) Identify optional data fields	6th Nov 30th Nov 31st Oct 31st Oct	
2) Y/N		a) Staff training on Octigo system b) Staff training on IG	30th Nov 1st Dec	LLBD Team LLBD Team
3) Y/N		a) Identify supplier has a documented Incident Management policy and recording system, and specify that any data breaches will be reported to DCC (data controller) b) Ensure individual login with password c) Ensure data can be amended by staff d) Set data validation on fields	6th Nov 30th Nov 6th Nov 6th Nov	LLBD Team LLBD Team LLBD Team LLBD Team
4) Y/N		a) Process for transfer to Stop Smoking database is documented b) Ensure data are securely stored with appropriate restricted access	30th Nov	
5) Y/N		a) Process for transfer to external services is documented b) Implement a DSA with health referral c) Ensure data are securely stored with appropriate restricted access	30th Nov 30th Nov 30th Nov	
6) Y/N		a) Ensure system is compliant with subject access requests and existing DCC policy and procedures b) Staff training on note taking	13th Nov 31st Dec	LLBD Team
7) Y/N		a) Identify Disaster Recovery plan and Certificate of Destruction b) Specify whether data will be deleted or returned at the end of the contract c) Include LLBD in PH retention schedules d) Include right to deletion in privacy notice	30th Nov 30th Nov 31st Dec 6th Nov	LLBD Team LLBD Team

Contact for future privacy concerns

Appendix 1 – Example Privacy Notice at Client Opt-In Stage

At Derbyshire County Council we take your privacy seriously and we want to be clear about why we are asking you for this information and how it will be used.

Why do we collect personal data about you?

We are asking you for this information so that we can provide appropriate and tailored wellbeing services to you. These services can be provided by Derbyshire County Council Live Life Better teams or by partner organisations:

We will also use monitoring data to evaluate the effectiveness of our wellbeing services but this will not include personal details.

How do we protect and process your data?

Any data we collect from you is stored electronically on a secure, encrypted system managed by our accredited data processor LGSS Shared Services, 4 Angel Street, Northampton, NN1 1ED. Derbyshire County Council is the data controller.

Safeguards are in place to ensure that both Derbyshire County Council and LGSS Shared Services adhere to the principles of the Data Protection Act 1998 regarding the correct handling, use, storage, retention and disposal of information. We make every effort to keep your personal data accurate and can update or correct records with any data you choose to share with us. We keep personal data for no longer than is necessary as required by law. Find out more about how we look after your information (opens in a new window https://www.derbyshire.gov.uk/working_for_us/data/)

When will we share data?

Your personal data are only seen by staff who need the information to do their job, such as the Live Life Better advisors. We do not publish personal data.

If you are referred to a service not provided by Derbyshire County Council we will need to share your data with them so you can be contacted. We will only share the minimum amount of information needed to access the service.

Derbyshire County Council only ever discloses information if explicit consent has been given by the individual(s), or when there is a clear legal basis to do so, for example, to protect a person from suffering significant harm.

Your rights

It is your right to request a copy of the information that we hold about you. Please contact the access to information officer:

Email: access2info@derbyshire.gov.uk, Telephone: 01629 538373 or Write to:
Access to Information Officer, County Hall, Smedley Street, Matlock, DE4 3AG

You are entitled to opt out of Derbyshire County Live Life Better service receiving or holding your personal identifiable information but this may stop us delivering a service to

you. There are also occasions where service providers will have a legal duty to share information, for example for safeguarding or criminal issues. The process for opting out will depend on which data and programme it relates to. For further information, please contact the Live Life Better team:

Find out more about your information rights from the Information Commissioner's Office (opens in a new window)

Terms & Conditions

Why do we collect personal data about you?
We collect personal data from you for the purpose of providing wellbeing services to you. These services can be provided by a range of partner organisations which could include, but are not limited to:

Relevant Northamptonshire County Council teams
Relevant Health professionals
Relevant local organisations

We will use the information to identify and make referrals to appropriate services; to monitor our work; to report on progress made; and to fulfil our statutory obligations and statutory returns as set by the law. The primary data owner will be First for Wellbeing.

How FFW protects and uses your personal data?
All personal data we collect from you complies with the data protection principles, as stated in the Data Protection Act 1998 (DPA) and NCCs Data Protection Registration with the Information Commissioners Office; for full list please check this website: https://ico.org.uk/ESDWebPages/DoSearch?reg=165079

The personal data we collect may be held as an electronic record on data systems managed by First for Wellbeing (FFW) or as a paper record. The records are only seen by staff who need the personal data so they can do their job. The security of the data follows FFW policies on Information Management. We make every effort to keep your personal data accurate. If you tell us of any changes in your circumstances, we can update the records with the personal data you choose to share with us.

We will keep the personal data for no longer than is necessary. Sometimes, the law sets the length of time personal data must be kept.

Sharing personal data
So we can provide the right services at the right level, we may share your personal data within county council services or with relevant organisations in line with FFW data registration, please see link above. Where this is necessary we will comply with all aspects of the Data Protection Act 1998.

Your rights
You have the right to ask us to stop processing your personal data in relation to any FFW service. However, this may stop us delivering a service to you. Where possible, we will do as you ask, but we may need to hold or process personal data to comply with a legal requirement. If you find that the personal data that we hold is no longer accurate, you have the right to have this corrected. Please contact the service holding the personal data or our Customer Services Centre for this.

Further information
If you would like further information about the personal data we hold or if you have a complaint about how your personal data has been used, please contact us at info@firstforwellbeing.co.uk with an email titled Freedom of Information and Data Protection.