Information Security Document

Joint Case Management System Privacy Impact Assessment

Version 0.2

Version History			
Version	**Date**	**Detail**	**Author**
0.1	12/02/2018	First Draft	
0.2	29/03/2018	Second Draft	
0.3	17/05/2018	Final Review and Board Sign off	
0.3		Review by IGG	
0.4		Further amendments	

CONTENTS

Section 1 - Privacy Impact Assessment Screening Questions

Will the project involve the collection of new information about individuals?	NO
Will the project compel individuals to provide information about themselves?	YES
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	NO
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	NO
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.	NO
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	YES
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.	YES
Will the project require you to contact individuals in ways that they may find intrusive?	YES

Section 2 - Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal.
Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The Council currently uses a workflow based case management system called Frameworki, provided by Servelec Corelogic, which provides a platform for initiating work and recording interventions to ensure compliance with statutory requirements to deliver social care for both adults and children. The system is hosted in-house. In Children's Services it is also the solution to support early help and intervention services delivered through Multi-Agency Teams. The system also enables non-statutory work, such as welfare rights, to be recorded comprehensively. It is the prime system used in both departments to record assessments and resources provided to individual clients. In Adult Care this includes the production of costed care packages and the ability to forecast net and gross expenditure in current and future financial years. This is a business critical system for both service departments.

On 2 February 2016 Cabinet gave approval to commence a procurement exercise for a joint Adult Care and Children's Services case management system using the CCS Framework. Additionally, the Council were able to include optional requirements for other Children's Services case work areas and a portal for use by professionals and clients, all of which would integrate with the core product. These options may be taken up at any point throughout the life of the contract, subject to further business cases and approval by Members. The new contract with Servelec Corelogic commenced on 22nd April 2017.

To meet customer requirements and to capitalise on general technological developments, Servelec Corelogic developed a new and improved system called Mosaic. All customers are expected to move to Mosaic, as support for Frameworki will be ceasing; work on the conversion process is currently underway.

Mosaic will provide enhancements and new functionality that can be exploited across both service departments. As well as re-procuring functionality that is already utilised, both departments are keen to explore new functionality and enhancements, including interfacing with other systems such as the Adult Care Scheduling and Activity Recording system (currently subject to

contract negotiations) and the Early Years and Education MIS system for Children's Services (currently in the process of being re-tendered). These interfaces will help to enhance and streamline existing work processes across the numerous departmental work areas.

Other aims and benefits include:

- To improve decision making by utilising one solution, delivered on one platform by bringing information together, complete with history and family context.
- To provide a fit for purpose system to support statutory and non-statutory services across Adult Care and Children's Services.
- Improved visibility of other agencies working with clients and their families.
- Improved service delivery standards.
- Comprehensive data security management by ensuring that information is shared in a targeted way, by only making information available to those practitioners who really need it.
- Improved data integrity, data quality and accuracy.
- Flexible and robust reporting and analysis.
- Enhanced safeguarding and protection of vulnerable adults and children, by ensuring that all the information known about an adult, child or family is available in one place, and to appropriate professionals.
- Flexible and mobile working from any location.
- Supporting collaboration with families and other agencies/voluntary sector/partners.
- Improved visibility of other agencies working with an adult, child or family.
- Auditing of activity to ensure that any breach or misuse can be fully tracked.
- The provision of a flexible platform that can be reconfigured and easily changed to reflect changes in legislation, service practice or organisational restructures.
- Use of the system by all staff, partners, agencies and potentially the public in a flexible and configurable manner, within and ideally beyond Derbyshire's administrative borders.
- To provide a fully integrated and flexible finance module to support end to end case management for both Adults and Children's social care and partner organisations.

The need for a PIA has been identified due to the personal information that is required to be collected and stored, of both adults, children, carers and family carers.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

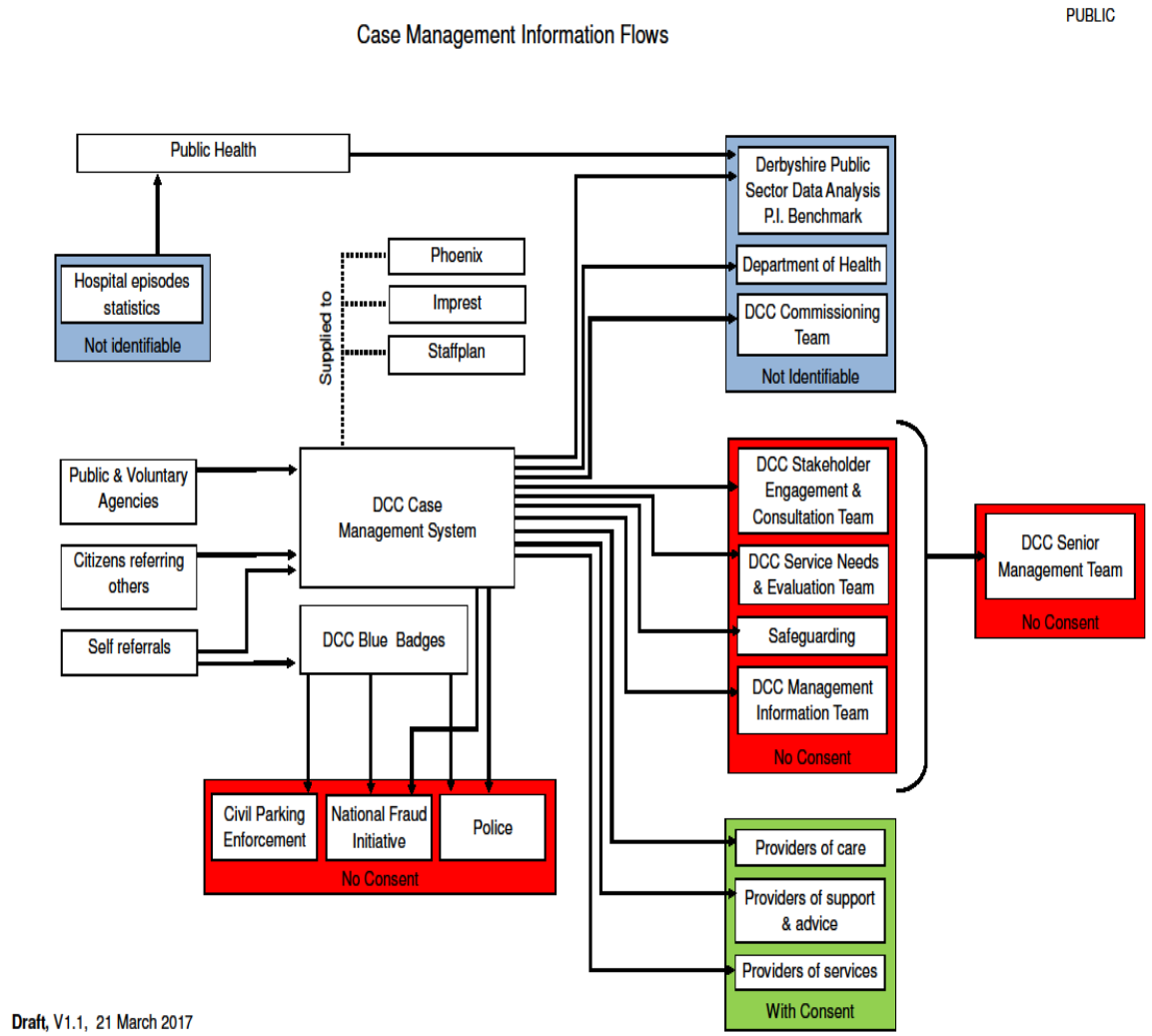
The collection of personal data is obtained from a variety of sources including self-referrals, clients, their carers and families, both statutory and non-statutory agencies and on occasions by members of the public who are concerned for the welfare and vulnerability of a local person. The data collected is both confidential and personal in nature; examples include names, addresses, date of birth and NHS number, as well as GP details. Some of the data is considered to be sensitive as defined by GDPR.

The data is accessed via the front end of Mosaic, and is controlled by assigning role-based access permissions to the system users. Users include external agencies from Health and Barnardo's. It is the responsibility of Adult Care and Children's Services to determine who should have appropriate role based access to view or amend the data.

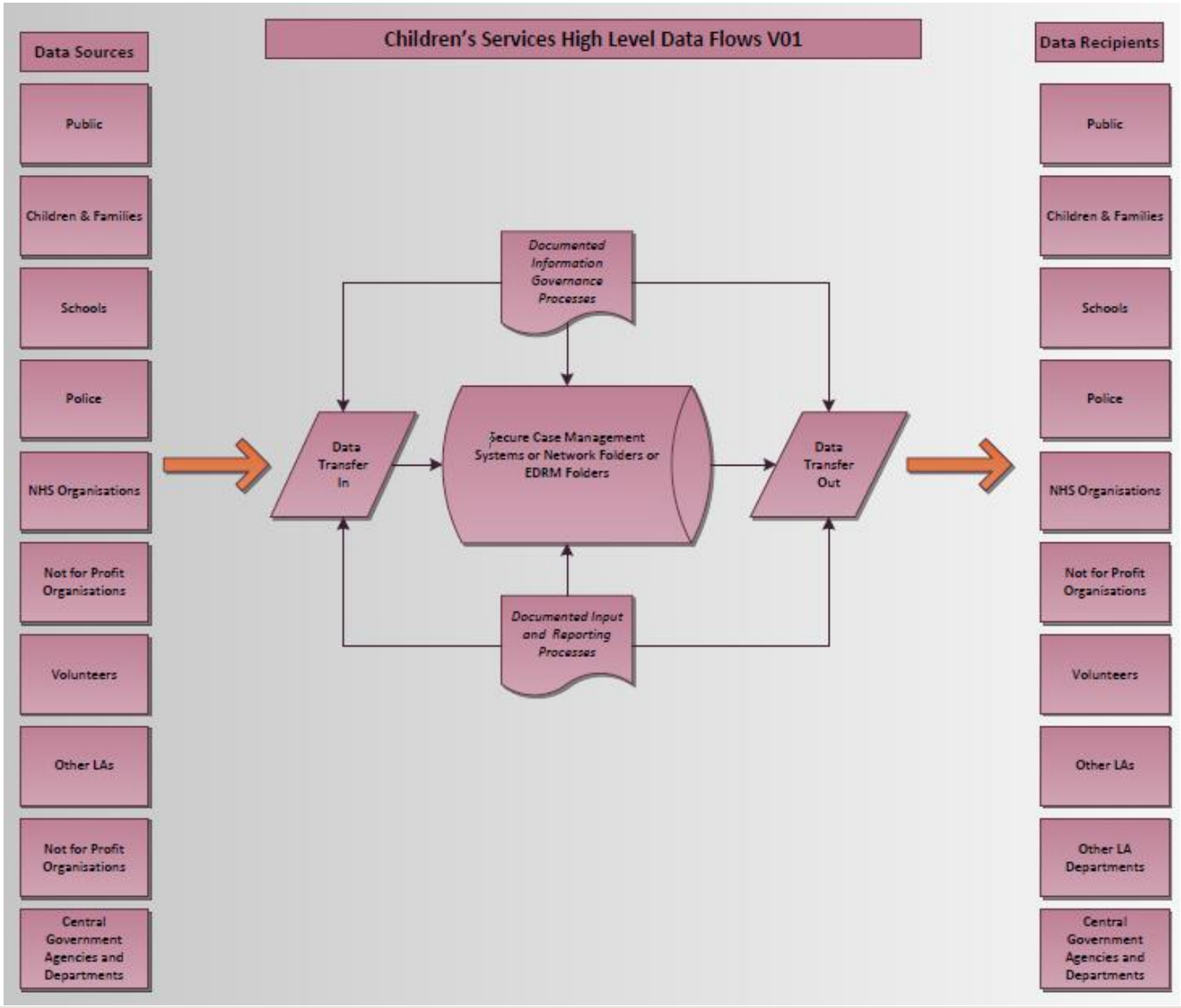
Data from the system is used to source the requirements of a number of Central Government Statutory Returns and the regulatory inspection frameworks of Ofsted.

The diagrams below illustrate the flow of information between users, Mosaic and associated systems.

Adult Care


PUBLIC
Case Management Information Flows
Public Health
Hospital episodes statistics
Not identifiable
Supplied to
Phoenix
Imprest
Staffplan
Derbyshire Public Sector Data Analysis P.I. Benchmark
Department of Health
DCC Commissioning Team
Not Identifiable
Public & Voluntary Agencies
Citizens referring others
Self referrals
DCC Case Management System
DCC Blue Badges
DCC Stakeholder Engagement & Consultation Team
DCC Service Needs & Evaluation Team
Safeguarding
DCC Management Information Team
No Consent
DCC Senior Management Team
No Consent
Civil Parking Enforcement
National Fraud Initiative
Police
No Consent
Providers of care
Providers of support & advice
Providers of services
With Consent
Draft, V1.1, 21 March 2017

Children's Services



Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

A project board has been established, which is led by two Service Directors from Adult Care and Children's Services. The project board is responsible for a number of aims and objectives, including dealing with any risks/issues, ensuring that there is a cohesive approach in meeting the overall aims of the project and setting and monitoring the delivery of the identified priorities. This board will also own the PIA and risks/mitigations identified.

Consultation will continue to be undertaken with all Adult Care and Children's Services work areas that use the existing system. A stakeholder and communications document has been produced which identifies managers and users across both departments and the methods of communication to be used throughout the project.

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

Data sharing agreements with partner organisations are developed by both service departments.

Additionally, privacy risks are constantly managed and monitored through compliance of PSN, ISO27001, system security, staff contracts and professional standards, as well as IG training.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
Section 3 can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
System 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.	Breach of Principle 7 of the Data Protection Act.	Financial and reputational damage. Legal action could be taken against the LA and possible substantial fine.
If a retention period is not established information might be used for longer than necessary.	Data becomes out of date and could be inaccurate.	Breach of Data Protection Principles 4 and 5.	Financial and reputational damage.
Data collection, storage and processing creates a risk of confidential information being accessed without the	An individual's privacy is compromised and data is shared beyond the organisation that the subject does not expect.	Reliance on all organisations to comply with data sharing agreements.	Reputational damage.

knowledge or consent of the adult, child/young person.			
Ensuring data subjects, i.e. an adult, child/ younger person, are aware of rights under data protection legislation relating to processing of data for these requirements.	An individual's privacy is compromised by breaching rights of a data subject in relation to their personal data, including right to withdraw consent.	Breach of Principle 6 of the Data Protection Act.	Reputational damage and potential fines.
System 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	Breach of Principles 3 and 4 of the Data Protection Act	Reputational damage and potential fines.

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
System data is accessed by unauthorised persons and used or shared inappropriately.	Access to the system will be limited to only those with the correct role based access activity. Role based access permissions are managed and controlled by the service departments. The use of the system will be managed locally through relevant training and guidance to practitioners.	Accepted/Reduced	
If a retention period is not established information might be used for longer than necessary.	The information will be stored within the system/archive in accordance with the Council's Records Retention Schedule. Any data that has met the retention expiry date will be deleted.	Accepted/Reduced	

Data collection, storage and processing creates a risk of confidential information being accessed/shared without the knowledge or consent of the adult, child/young person.	The Children's Act 1989, 2004 and Human Rights Act 1998, Care Act 2014 in addition to other policy drivers have been consulted to ensure that consent to share any adult or child information would not breach any confidentiality or privacy issues, where it is deemed necessary to share the information.	Accepted/Reduced	
To ensure data subjects are aware of their rights regarding their personal data, including their right to withdraw consent at any time and the process for doing so.	All Local Authority Privacy Notices will be updated to reflect any system changes and ensure they cover the rights of data subjects in relation to the personal information it holds about them. All clients will be referred to these Privacy Notices. Where consent is deemed to be necessary, all consent forms used to collect personal data used by the Local Authority will be compliant with the new GDPR regulations and will refer to rights of data subjects, including right to withdraw consent and the process for doing so.	Accepted/Reduced	
System data is inaccurate at the point of collection/data entry or subsequently becomes	Where appropriate, verification processes are undertaken such as checking birth certificates. Training of system users.	Accepted/Reduced	

inaccurate by being out of date	Case file audits. Validation against other external systems such as NHS spine. Configuration of the system to promote and support data integrity.		

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As outlined in step 4	As outlined in step 4	

Step six: 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
Project Governance and controls including highlight reports to be completed during the life span of the project.	Ongoing	Project Team (Adults and Childrens)

Testing of technical solutions and controls before ‘Go-Live’. Oversight and evaluation of the project against the success criteria.	Late June 2018 Post Go-Live	Project Board
Contact point for future privacy concerns David Gurney/Chris Newton for escalation to the Project Board		

Section 3 - Linking the PIA to the Data Protection 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 DPA or other relevant legislation, for example the Human Rights Act.

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 Notices
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?	N/A
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?	No

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?	N/A

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?	Use of other systems to validate data – eg, NHS Spine and internal verification processes

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?	See Records Retention Schedule
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?	Yes
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?	Training for all users for the new system, delivered by the supplier, and via e-learning materials produced in-house and ongoing training for new starters via e-learning.

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