Data Protection Impact Assessment Report

Project Information	
Project Name (and or number)	LiquidLogic CMS
Business Area/s Affected	Families and Children's Service
Information Asset Owner	Lynda Cox
Senior Responsible Officer	Lucy Townsend
Project Manager	Beverley Elliott
Data Protection Officer	Andrew Holyoake

Document Ownership	
Author(s)	Lynda Cox
Document Owner	Lucy Townsend

Document Review Information			
Document Location			
Quality Reviewers	**Name**	**Role**	**Sections Reviewed**
Version History	**Version Date**	**Requestor of Change**	**Summary of Change(s)**
V1	November 8th 2018		

Data Protection Impact Assessment Report

1. Outline of the project, objectives and benefits

The project will introduce a new case management system to process and store the records associated with children and families' services. The system will replace the Council's own recording systems and allow easier information sharing across its services and teams.

The Council also wants to improve information sharing across its partners as this is often cited as the reason some cases do not have optimum outcomes. The aim is to allow partner agencies into part of the system to record early help assessments for children and young people at the same time as allowing other agencies access to add to that information. Agencies will also have parts of forms delegated to them to completed. This will be via portal access. We aim to operate a system that optimizes information sharing safely and consequently improve outcomes for children and families.

2. Describe the intended use of personal data:

a) Describe the nature of the processing:

- This project implements new software and database, portals.
- Data will be entered into the system through a mix of manual keying and data imports
- The system is a hosted database system
- Data are utilised to inform a variety of social care, and support service provision in children's social care, education and early help.
- Data is accessed by Council staff in relation to services provided, and some staff in partner organisations where a statutory basis or information sharing agreement exists.
- Data is shared with; partner organisations where a statutory basis or information sharing agreement exists.
- Retention periods across data are dependent on categories and are therefore variable but listed in the department retention schedule eg safeguarding or under rules in relation to enquiries into historical cases of child sexual abuse.
- Security measures include: - Role specific access permissions, 2-factor verification for external users, end user agreements, training (e-learning and face to fact), the Council's IG security suite.
- The sensitivity and size of database determine need for statutory DPIA

Information that will be stored in the case management system comes from many sources. Directly from the child/family, gathered by the council front line worker or by a professional from another agency.

Information will be recorded either via direct access to the system (either a council worker or a worker from a partner agency), by delegated form completion or via imports of information eg the census completed 3 times a year by schools or data supplied through Groupcall (an electronic file transfer system).

b) Describe the scope of the processing

Information is recorded in the case management system. It is largely personal information related to children 0-18 and their families. It is a mix on contextual, demographic data and case information used in many functions from childcare funding, school admissions, support for additional needs, support for social care and care leavers, support for early years settings and schools.

Data Collection will encompass recording a breadth of information, supporting a number of services including:

- demographic information for children and associated adults
- contact information for families of children.
- family information for children
- information professionals involved in cases for children
- information for early help and social care assessments
- information relating to child protection plans
- foster carer enquiries (demographic information)
- foster carer approval process
- adopter approval
- private foster carers
- information that relates to 'family life'
- information relating to harm or abuse of a child.
- information relating to possibility of Child Sexual Exploitation
- pregnancy/maternity information
- sensitive information regarding children & young people and safeguarding.
- information for purposes of court hearings and cases.
- personal information that could be used in panel meetings, reviews or case meetings.
- education information for children
- Free School Meals eligibility
- Manage School Exclusions and Reinstatement Process
- Tracking and Monitoring School Attendance
- Missing from Education
- Vulnerable Groups information
- Special Education Needs and EHCPs
- Manage & Support of Children in Entertainment
- Manage & Support Children in Employment
- Early Years free child care attendance and payments process
- Children’s Centres attendance
- School Admissions process

- Specialist Services including Visual and Hearing Support
- Tracking Educational Needs of Children in Care (Virtual School)
- Raising Participation Age & NEET tracking process
- Support to ethnic minority children and travellers
- Behaviour support
- Death Notification
- Information about Establishments and agencies
- Governors Information & Activities
- Manage Education Setting / Improvement: Attainment

At any one-time records of most of the population 0-17yr olds in Wiltshire will be held on the system (100k+) alongside additional connected adults. Some recording continues to age 25. Historical records are held according to retention schedules.

The data covers every category of special category data, and include the most sensitive records held by the authority.

The geographical area covered is UK with commonality of connection to geographical area of the county of Wiltshire.

Processing is 24/7, as emergency duty team cover outside of normal office hours.

Information tracks a child’s early years and school life and sometimes (eg for children in care) has very long retention period associated with it. Information is sensitive and carries all the necessary qualities of confidentiality.

Information covers mainly Wiltshire residents but will include children and families from outside the LA where those children attend Wiltshire Early Years settings or schools.

It covers a large proportion of the 0-17 population – 105,000 children and young people at any one time plus their associated adults. SEN and care leaver clients can still be engaged for support until the age of 25yrs.

c) Describe the context of the processing:

- the source of the data - internal staff, external staff of partner agencies, the families and data subjects themselves
- the nature of your relationship with the individuals - Service provider, with statutory relationships such as tracking & safeguarding
- the extent to which individuals have control over their data - negligible control relying on statutory rights only
- the extent to which individuals are likely to expect the processing – the vast majority of processing activity is open and transparent, covered by detailed privacy notices.
- Includes children or other vulnerable people

- This information type has previously been stored and processed by the Council. New advances include Delegate access by portals and direct sign on to parts of the system
- The system will be compliant with service specific government guidance on ways of working and Government data collection

Information is shared with many parties. For example, Children's case information may be shared with health professionals and health professionals may share information with us. There are teams that are using the existing data storage systems where information sharing is currently covered by an information sharing agreement.

All third parties who engaged with the CMS will be required to sign up to the Wiltshire Information Sharing Charter, as members, and to a specific personal information sharing agreement (PISA).

Information may be shared with other professionals working on the case and a summary could be provided to care providers.

Information may be shared between departments as necessary.

Information may be shared with other Local Authorities, where a child or adult open to Wiltshire services moves to another LA or is admitted to hospital in another LA, attends an educational establishment, moves to care provision outside of area or other relevant reason where information would need to be shared for the safety of a child or adult open to our services.

Information may be shared/passed between education establishments and the council.

Information may be shared with multiple agencies as required including charitable organisations and the police.

The processing of this type of data will be similar in every local authority with the involvement of partner agencies being a growing trend.

d) Describe the purposes of the processing:

The intention is to have a single system that enables us to meet statutory requirements across C&F services and create;

- An easier system for practitioners to use and to release time to spend on direct work
- A holistic view of the child and family
- Information sharing to be easier and more productive
- Better partnership engagement ensuring that services are co ordinated
- Because of the above, better outcomes for children and young people

3. Consultation:

a) The following consultation approach and stakeholder groups were incorporated into the consultation process:

Council staff have been consulted with as part of the procurement and set up of the new system. This includes practitioners and their managers and IG/ICT/security specialists. Multi-agency partners are being consulted about their direct engagement with the system.

b) A summary of the stakeholder views are as follows:

Staff are welcoming the new system and the improved way of working that it will bring.

Partner agencies have been consulted through the FACT Board and via a variety of events to get their views on engagement and future third-party use of the CMS system.

FACT is also consulting over the approach of co-production.

The above stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities.

4. Data protection compliance – assessment of necessity and proportionality of personal data processing.

Principle 1: Use of personal data is fair, lawful, and transparent:

Lawful basis for the processing of personal data is stated as follows:

- Personal data will be processed either with consent, to perform contract with data subjects, for legal obligation, for protection of data subject’s vital interests, performance of public interest task or for exercising official authority,
- Special Category data will be processed either with explicit consent, to protect vital interests of data subjects for legal claims or at direction of the courts, for the provision of social care or management of social care systems
- Criminal data will be processed in support of the prevention and detection of crime and the prosecution of offenders, in accordance with the Data Protection Act 2018.

How will individuals be made aware of the processing - Data Subject Information Notices at point of collection and published Privacy Notices.

Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:

Information is collected in line with statutory guidance and legal basis, for operational and strategic use and for reporting to central government.

Principle 3: Use of personal data is adequate, relevant and no more than necessary:

Liquidlogic's premise is to collect into one database a holistic view, and negate multiple and duplicated records across wider storage. This is key to minimising the data held. Compliance with this principle relies upon professional judgement building on minimum statutory requirements.

Principle 4: Personal data must be accurate and kept up to date:

Accuracy of data will be maintained by professionals gathering data when working with children and families and via their connections with partner agencies. Data quality will be tested by managers via supervision and by the systems team through data quality work.

Imports of information from settings will enable demographic information to be kept up to date.

Information will either be allowed to be corrected/amended/updated by the front-line worker or by the system admin team. LiquidLogic may be involved in some of this work. Customers who disagree with recording will have their views kept on the system as well as the professionals view of the data.

Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:

These electronic records will be retained no longer that is required by statute or legal obligation

Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:

IG Security measures as approved by Information Security Lead

End user agreements which include an integrity statement are signed for all users, appropriate IG training for all users.

7. Personal data will be processed in accordance with the individual's data protection rights:

How will requests from individuals wanting to exercise their rights be managed - All staff made aware by mandatory training that all data subject's rights referrals should be passed to IG team to deal with in conjunction with service.

8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:

Personal data is not being processed outside the EEA.

9. The council must be able to demonstrate how they are complying with the Data Protection Act 2018 & GDPR:

GDPR and DPA 2018 compliance will be assured. Requirements for NHS data security and protection toolkit will provide evidence together with existing policies and procedures.

5. Identifying and assessing risks

The focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix.

	Describe the <u>source</u> of the risk, the <u>problem</u> it creates and the <u>potential impact</u> on individuals. Focus on data protection compliance risks. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, significant or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium or high.
1	Inappropriate access to system E.g. Sharing passwords, Accessing information with no business need Illegal penetration	possible	significant	medium	Log in page says do not share passwords 2 Factor authentications in place for external users meaning access code sent to one person End user agreement signed by all users that confirm they will only access information when a business need is in place Routine audits look for evidence of workers accessing records inappropriately LL use penetration testing to highlight any weakness to external attack	All HOS (FCS)	low

	Describe the source of the risk, the problem it creates and the potential impact on individuals. Focus on data protection compliance risks. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, significant or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium or high.
2	Security breach E.g. Information disclosed inappropriately Information sent to wrong client	possible	significant	medium	Practitioners professional training supports appropriate information sharing Managers supervision advises practitioners around appropriate information sharing Council IG e-learning reinforces appropriate behaviour Regular reminders about care /extra checks needing to be taken, double enveloping etc to mitigate against human error Workers advised to check a source document for client's current address	All HOS (FCS)	medium
3	Information stored/recorded is not accurate or up to date E.g. Information wrongly entered or not entered at all/in a timely way Information out of date but correct at last update Decision making based on poor information	possible	significant	medium	Managers check that workers are recording in an accurate and timely manner. Audit highlights any issues relating to recording and the need to improve. Workers are expected to keep their recording up to date Cross checking of accuracy of facts when decision making	All HOS (FCS)	low

	Describe the source of the risk, the problem it creates and the potential impact on individuals. Focus on data protection compliance risks. Mention corporate risks only as necessary.	**Likelihood of harm** Remote, possible or probable.	**Severity of harm** Minimal, significant or severe.	**Risk score** Low, medium or high.	**Agreed action** Detail to action that will reduce the risk	**Action Owner & due date** Name & date	**Residual Risk score** Low, medium or high.
4	Misuse of data by users	Possible	Significant	Medium	Mandatory staff training and regular sampling and monitoring of processing activity, aligned to potential disciplinary actions for detected misuse will act as significant disincentive. HR policies already allow for this. However, the risk can never be completely removed.		Low

***If you have accepted any of the above risks you must provide a rationale for doing so in the 'Agreed Actions' column.**

6. Authorisation of DPIA:

DPIA copies will be retained by the DPO, Information Asset Owner and within the relevant Project Management records.

a) Approval signatories

Item	Name / role / date	Notes
Risk Reducing Measures approved by **Information Asset Owner:**	Lynda Cox	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by **Senior Responsible Officer**:	Lucy Townsend [redacted]	Acceptance of mitigating actions.
Data Protection Officer approval of DPIA:	Andrew Holyoake [redacted]	DPO should consider any medium / high residual risks and whether processing can proceed
Summary of DPO advice: Keep this document under review and up to date as use of the system develops.		

b) Residual high risks (complete <u>only</u> if there are any ‘high’ <u>residual</u> risks):

Item	Name / role / date	Notes
DPO advice accepted or overruled by **Senior Information Risk Owner (SIRO):**		If overruling the DPO’s advice you should record your rationale below
SIRO Comments:		
Date and name of person referring DPIA to ICO:		As required by law if any high residual risks remain.
Summary of ICO advice:		

c) Accountability – update of ‘records of processing’:

Information Management Name / role	Information Asset Register	Special Category Data Policy Document	Notes
			Add dates the records were updated.

d) Review of DPIA:

Item	Information Management Name / role / date	Frequency	Notes
DPIA will be kept under review by:	Lynda Cox	1/4ly whilst development project is still running	Review April 2019